Forberedelse og datakriminalitet

Forebygging av angrep mot infrastrukturen

Kandidatnummer: 564

Leveringsfrist: 26. november

Til sammen 15 948 ord

08.07.2008

Innholdsfortegnelse

1 INNLEDNING

1.1 Tema og problemstilling

I denne oppgaven skal jeg se på lovverket rundt vern av data og informasjonsutveksling. Jeg skal vurdere om det er ønskelig å utvide straffeansvaret innenfor dette rettsområdet, slik at flere handlinger av forberedende art blir straffbare. Selv om det er et prinsipp i norsk rett at forberedende handlinger ikke er kriminelle, foreligger det i dag en rekke unntak. Dette gjelder handlinger som er vurdert som spesielt farlige eller uønskede. Slike handlinger er kriminalisert allerede på det forberedende stadiet, som en forebyggende strategi. Jeg skal vurdere om dette kan være en god løsning også innen rettsområdet data.

Arbeidet med den nye straffelovens spesielle del pågår for tiden i Stortinget. Det er foreslått av flere instanser å innta et eget kapittel om vern av data, informasjon og informasjonsutveksling[1] i denne delen. Dette er fordi straffebudene som skal verne om datateknologien beskytter helt andre interesser enn andre straffebud gjør. Den digitale verden medfører egne behov for beskyttelse som skiller seg fra de behov som ellers gjør seg gjeldende. Disse behovene er satt på dagsordenen i sammenheng med arbeidet med den nye straffeloven. Dette er også blitt satt under søkelyset internasjonalt. Datakriminalitet er nemlig typisk internasjonal kriminalitet, og forutsetter internasjonalt samarbeid.

[1] Forslått første gang i NOU 1985:31

Norge undertegnet 23 november 2001 Europarådets Konvensjon om datakriminalitet[2]. Denne inneholder regler om vern av data og informasjonsteknologien. Denne ble ratifisert og vedtatt 4 november 2005.
Konvensjonen inneholder også noen bestemmelser av forberedende art. Dette gjelder nærmere definert forskjellige former for befatning med datateknologi som er særlig utviklet eller tilpasset til å begå brudd på de andre straffebudene i konvensjonen. Det var imidlertid anledning til å reservere seg mot deler av denne. Norge valgte å reservere seg der dette var mulig.

I denne oppgaven skal jeg altså se på hvorvidt vi burde inkorporere resten av disse forberedende handlingene i norsk rett, og i så fall i hvilke former dette bør utformes.

1.2 **Datakriminalitet**

Utvilklingen innen datateknologien kan sammenlignes med den industrielle revolusjon når det gjelder den betydning den har hatt for enkeltindivider og organisasjoner[3]. Noen av likhetstrekkene som kan nevnes er utviklingen av ny teknologi, utbredelsen av denne teknologien og erstatning av menneskekraft med megabyte.

Ordet datakriminalitet er det mest vanlige i Norge, men internasjonalt er det ordet cybercrime og andre engelske uttrykk som blir brukt. Derfor brukes disse termene mye i den videre drøftelse. Datakriminalitet omfatter altså all kriminalitet hvor data eller nettverk brukes som mål, middel eller arena for kriminelle handlinger. Det begrenser seg således ikke kun til handlinger hvor data er målet for handlingen, som dataskadeverk eller datatyveri. Uttrykket favner alle kriminelle handlinger, så lenge data er en del av handlingen.

---

[2] Se conventions.coe.int, samt vedlegg 1

[3] En sammenligning som ble gjort i NOU 2007:2

Datasystemer brukes ikke bare privat og i arbeidssammenheng, men også i det offentlige. Fra år 2000 til 2005 har bruken av Internett økt med 170 %[4]. Dette skyldes offentlige innretninger, internasjonale og nasjonale organisasjoner, næringsvirksomhet og enkeltindivider. 77 % av de som har benyttet Internettet har brukt det til finansielle tjenester, som nettbank.
86 % av befolkningen bruker e-post. Vi bruker mer e-post og leser aviser på nettet, enn vi bruker papirversjonene. Når det gjelde bedrifter er mer enn 90 % Internett-tilkoplet og bruker dette i hverdagen.
Mange bruker mobiltelefon i stor utstrekning. Denne har tatt over for bruken av fasttelefon. Mobiltelefonen er mer utsatt for angrep.
I butikken bruker de fleste betalingskort i stedet for kontanter. Mange handler også direkte over Internettet. Vi signerer elektronisk, og vi identifiserer oss med elektroniske midler. Sensitive opplysninger om personer, bedrifter og banker svever gjennom dette offentlige rommet kalt cyberspace.

Av 3900 anslåtte datainnbrudd er kun 61 anmeldt. Dette kan være fordi saken oppfattes som ubetydelig, og man ikke har tro på at det er mulig å finne gjerningsmannen. Mange tror ikke at politiet har kompetanse eller ressurser til å oppklare slike saker, og dette kan stemme i varierende grad. I tillegg føler mange at anmeldelse er for ressurskrevende[5].
De vanligste kriminelle handlingene innen data er datainnbrudd, dataskadeverk (tjenestenektangrep), datatyveri (ID-tyveri), databedrageri (nettbankbedragerier) og ulovlig fildeling[6]. Dette er områder som Kripos og politiet jobber mest med å løse.
Dette er også handlinger som rammes av konvensjonens bestemmelser, og som videreføres i den norske straffeloven.
Nye metoder utvikles og tas i bruk. Metoder som botnets[7], phishing[8], pharming[9], spyware[10], spam[11] og identity-theft[12] er globale uttrykk som har kommet til de siste årene.

---

[4] tallene er hentet fra ”Mørketallsundersøkelsen 2006”, Næringslivets sikkerhetsråd, www.nsr-org.no

[5] *Næringslivets Sikkerhetsråd, 2006*

[6] opplysning fra besøk av Kripos, ved Berit Børset Solstad

Dette er metoder som utnytter de svakheter som finnes i datasystemer. Kriminelle handlinger som alltid har funnet sted, som tyverier, omsetning av tyvegods og pengefalsk, har fått nye marked og nye metoder for gjennomføring.

Dette gjør oss selvfølgelig sårbare. Med rask utvikling kommer også nye arenaer for kriminelle. Nye metoder for kriminell virksomhet, og nye metoder for å gjennomføre denne. Internettet er åpent for alle, med liten oversikt over hvem som befinner seg hvor og når. Med alle transaksjoner og personlig informasjon løpende gjennom dette offentlige rommet finnes det metoder for de kriminelle å fange opp disse på veien.

---

[7] definisjon fra Wikipedia.com : **Botnet** is a jargon term for a collection of software robots, or bots, which run autonomously and automatically. They run on groups of "zombie" computers controlled remotely by crackers. This can also refer to the network of computers using distributed computing software.
While the term "botnet" can be used to refer to any group of bots, such as IRC bots, the word is generally used to refer to a collection of compromised computers (called zombie computers) running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure. A botnet's originator (aka "bot herder") can control the group remotely, usually through a means such as IRC, and usually for nefarious purposes.

[8] In computing, **phishing** is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay, PayPal and online banks are common targets. Phishing is typically carried out by email or instant messaging,[1] and often directs users to enter details at a website, although phone contact has also been used.[2] Phishing is an example of social engineering techniques used to fool users.[3

[9] **Pharming** (pronounced farming) is a cracker's attack aiming to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.

[10] **Spyware** is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

[11] Spam (electronic), unsolicited or undesired bulk electronic messages.

[12] Identitets-tyveri

Det vanligste motivet bak slike handlinger er ønsket om spenning. Mange ønsker ikke nødvendigvis noen profitt, men vil bevise at de besitter den kunnskap som skal til, og ønsker å se hva som skjer dersom de gjennomfører handlingen. Det starter ofte med at man laster ned programmer fra Internett, som gjør det mulig å entre datasystemer uten den rette autorisasjon. Etter kort tid lærer man hvordan man kan lage ormer og slikt selv.
Status er et viktig motiv, mange opererer gjerne i et miljø hvor det er spennende å se hvem som klarer å entre flest sikkerhetsklarerte systemer og flest viktige systemer. Det er for eksempel spennende å se hvem i miljøet som klarer å overstyre flest maskiner på en gang i et botnet. Dette kan også brukes til å spre propaganda.
Det utvikles miljøer innen dette feltet som i andre sammenhenger, og det er ikke uvanlig at to ”gjenger” går mot hverandre for å se hvem som er sterkest ved å forsøke å ta over den andres nettverk. Dette rammer mange uskyldige som er fanget i dette nettet.
Ønske om hevn kan være et motiv, for eksempel for en eks-ansatt som ønsker å gjøre ting vanskelig for bedriften.
Ellers er selvfølgelig profitt vanlig motiv.

Det foreligger en stor trussel, selv om det ikke er dokumentert at det noen gang har skjedd, for at informasjonskrigere kan få meget sensitiv informasjon om et annet land. Dette er informasjonsjegere som entrer sider fra et lands myndigheter og militære, for å drive en ulovlig etterretning.

Her er noen definisjoner som gjør det lettere på veien videre:
Cyberspace[13] en infrastruktur av datasystemer i nettverk, der flere datasystemer møtes til et felles rom.

[13]**Cyberspace** is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.
Definisjoner fra wikipedia.com

Datasystemer er definert som enhver innretning eller gruppe innretninger, som er koplet sammen eller som hører sammen, hvorav en eller flere utfører programmert, automatisk behandling av data. [14]

Cybercrime[15], eller datakriminalitet, omfatter enhver kriminell handling hvor data brukes som mål eller middel.

Cyberattack[16] et samordnet angrep på et nettverk eller datasystemer ved å utnytte dets svakheter.

1.3 Cyberterrorism

Internasjonalt foregår det mye arbeid med bekjempelse og forebygging av terrorisme. Et grunnleggende spørsmål, som er gjenstand for mye debatt, er derfor hvordan man skal definere ordet "terrorisme". Dette er et ord som forskjellige nasjoner, områder og folkeslag kan ha forskjellige oppfatninger av. En definisjon av terrorisme er at det innebærer en handling, begått av en gruppe eller enkeltpersoner, av politiske eller ideologiske grunner, rettet mot sivile deler av en befolkning, i den hensikt å skape frykt og terror. Formålet er å kapre oppmerksomheten fra de sivile og styresmaktene rundt en ideologi, og de sivile blir brukt som "gisler" for å oppnå forhandlinger eller kun den oppmerksomhet som ønskes[17].

---

[14] definisjon fra Ot. Prp. Nr. 40 (2004-2005) s 40

[15] cybercrime – a term used broadly to describe acticity in which computers or networks are a tool, a target or a place of criminal activity.

[16] wikipedia.com : Many current computer systems have only limited security precautions in place. This **computer insecurity** article describes the current battlefield of computer security exploits and defenses

[17] Definisjon fra Wikipedia.com: **Terrorism** in the modern sense[1] is violence or other harmful acts committed (or threatened) against civilians for political or other ideological goals.[2] Most definitions of terrorism include only those acts which are intended to create fear or "terror", are perpetrated for an ideological goal (as opposed to a lone attack), and deliberately target or disregard the safety of non-combatants. Many definitions also include only acts of unlawful violence.

Dette leder til spørsmålet om hva cyberterrorism er. Dette kan defineres som en gjennomføring av en terrorhandling ved hjelp av et cyberattack. Et cyberattack, som definert over, er et organisert og samlet angrep på cyberspace eller et datasystem. Et slikt angrep kan oppfylle alle kriteriene for å kvalifisere som terrorisme. Terrorisme gjennom cyberattack er altså cyberterrorism, eller cyberkrig. Her er Gartners definisjon av cyberkrig: "Handlinger understøttet av en stat mot en motstander der hensikten er å overta kontrollen over eller forvrenge all slags informasjon: Innhold, støttesystemer og programvare, det fysiske utstyr som lagrer data eller instruksjoner, samt menneskelige samarbeidsformer og oppfatninger[18]."

Et systematisert og organisert angrep gjennom cyberspace eller på datasystemene ville vise den ytterste grad av vår sårbarhet. Et slikt angrep ville kunne sette et samfunn ut av spill, og å lamme det. Et cyberattack ville kunne føre til de konsekvenser som er ønsket for terrorister, selv om det ikke innebærer fysiske bomber og blodbad. Ordet terror omfatter mye mer en datarelaterte forbrytelser, men man kan si det slik at den ytterste form for datarelaterte forbrytelser er terrorhandlinger.

Et slikt angrep er enda ikke dokumentert å ha funnet sted, men det er dokumentert tilfeller som har skapt lignede effekter. Et eksempel er angrepet på Estland i september 2007. Dette angrepet er det mest omfattende og det mest velorganiserte angrep gjennom cyberspace som verden noen gang har sett. Det spekuleres således i om dette var et organisert angrep fra en fiendtlig stat eller organisasjon, ettersom det var så bredt, velplanlagt og foregikk på så mange fronter. Målet var banker, departementer, aviser, kringkasting og telefonsentraler. De viktigste delene i nasjonens infrastruktur ble angrepet. En stund var også nødnumrene ute av drift. Avanserte metoder ble tatt i bruk, stadig nye mål ble angrepet og svakheter ble utnyttet etter hvert som de oppsto. I følge rapporter var det i visse perioder over en million "fangede" maskiner i bruk. Ingen skjønte helt hva som skjedde, men datasystemene var ute

[18] Gartner, referert til gjennom artikkel skrevet av Peter Hidas utgitt på siden til idg.no

av stand til å ta imot kommandoer fra andre systemer. Derfor var det vanskelig å motreagere, fordi man ikke kom til i systemene for å reparere.

Spørsmålet videre er hvordan man kan forberede seg på slike angrep, og hvordan man kan forebygge at slikt skjer. Formålet er å begrense skade, og å forebygge at det skjer. Dette er en tanke som har vunnet plass i flere land, i Europa og ellers i verden. Den ligger til grunn for Europarådets konvensjon om cybercrime[19], som oppfordrer alle til å gjennomføre et lovverk for å harmoniserer kampen mot datakriminalitet. Den inneholder noen bestemmelser av forberedende art.

Senere kom Europarådets konvensjon om bekjempelsen av terror[20], i 2005. Denne inneholder regler om forebygging av terror, med og uten bruk av datakriminalitet. Denne har Norge ikke signert. Dersom alle landene harmoniserer sine regler på dette området vil man lettere kunne begrense slik kriminalitet. Det er viktig å ha et regelverk som er effektivt innen dette feltet. Man kan snakke om lov og orden i cyberspace, som en parallell til lov og orden i samfunnet for øvrig. Det er et eget samfunn vi snakker om her, som medfører egne utfordringer.

[19] Convention on Cybercrime (lovtiltak mot datakriminalitet), vedlegg 1, se www.conventions.coe.int

[20] Council of Europe Convention on the Prevention og Terrorism, vedlegg 2, se www.conventions.coe.int

2 AVGRENSNING AV OPPGAVEN OG DRØFTELSEN VIDERE

2.1 Avgrensning av oppgaven

Denne oppgaven handler om hvorvidt norsk lov bør utvide straffeansvaret innen datakriminalitet, slik at forberedelseshandlinger omfattes som selvstendige straffebud. Jeg vil ikke gå detaljert inn på grensen mellom hva som utgjør straffri forberedelse og hva som utgjør straffbart forsøk. De handlingene som konvensjonen anbefaler de signerende statene å ratifisere i nasjonal rett er uten tvil av forberedende art. Det er nettopp derfor de ikke allerede er straffbare etter forsøkbestemmelsen. De gjelder befatning med forskjellige typer midler som er anskaffet på en urettmessig måte og som skaper fare for overtredelse av andre straffebud. Dette problematiseres ikke videre.

Oppgaven handler altså om hvor langt forberedelsesansvaret bør rekke innenfor emnet datakriminalitet. Andre straffebud innenfor området skal ikke utredes noe videre. Det kommer frem av kapittel 3 hva som er gjeldende rett om cybercrime. Det er i stor grad bestemmelsene i konvensjonens art 2-5 som omhandler de selvstendige straffebudene innen cybercrime. Disse er altså dekket i norsk rett gjennom straffebud som er plassert forskjellige steder i loven. Denne uoversiktligheten gjør at jeg velger å referere til art 2-5 i konvensjonen når jeg omtaler disse handlingene, heller enn å ramse opp de forskjellige paragrafene som dekker disse i norsk rett.

Jeg avgrenser videre oppgaven mot spørsmålet om strafferammene for de forskjellige bestemmelsene. Dette er i høysete grad interessant, men faller noe utenfor det prinsipielle spørsmålet om hvor langt ansvaret bør rekke.

Jeg ser på terrorisme gjennom cyberattack i denne oppgaven. Utviklingen innen internasjonal forebygging av terrorisme kan ses som en parallell til utviklingen innen bekjempelsen av cybercrime. Begge dreier seg om forebygging og ramming av

forberedende handlinger. Ettersom terrorisme kan forekomme gjennom bruk av data er det interessant for denne oppgaven. Det kan tjene som eksempel på hvorfor prioritering og bekjempelse av cybercrime er så viktig. Cyberterrorism viser hvor sårbare vi er og hvilke konsekvenser cybercrime kan ha. Jeg skal altså ikke kartlegge hvordan rettstilstanden er når det gjelder bekjempelsen av terrorisme i Norge generelt, men skal kun befatte meg med datarelatert terrorisme, som en type datakriminalitet.

2.2 **Drøftelsen videre**

I innledningen har jeg skrevet litt om hvorfor forberedelseshandlinger innenfor området datakriminalitet er viktig og interessant. Jeg har skrevet litt om utbredelsen av data, og i forbindelse med dette litt om utbredelsen av datakriminalitet. Cyberterrorism tjener som det mest alvorlige eksempel på dette.

I den videre drøftelsen skal jeg først kartlegge gjeldende rett om datakriminalitet i dag, i kapittel 3. Etter oversikten over hvilke regler vi har om dette i dag, punkt 3.1, kommenterer jeg i hvilken grad forberedelseshandlinger innen datakriminalitet er kriminalisert, punkt 3.2. Videre kommer en oversikt over den utvikling som har skjedd de siste årene på dette feltet, i punkt 3.3, for å belyse den økende relevans dette emnet har fått. Den nyeste utredningen om dette, og lovforslaget som hører til, diskuteres i punkt 3.4. Til slutt kommer jeg i punkt 3.5 raskt inn på reglene rundt forebygging av cyberterrorism og hvilke endringer som står på trappene her.

I kapittel 4 kartlegger jeg fremmed rett. Jeg har valgt å begrense dette til internasjonale rett, svensk og dansk rett.. Den internasjonale retten er viktig fordi det hovedsakelig er her endringene har kommet til. Det er internasjonale organisasjoner som har vært pådrivere for en harmonisering av regelverket i Europa. De regler som er drevet frem her er signert av statene, og de har forpliktet seg til å ratifisere reglene. Det mest interessante for Norge er hvordan de landene vi identifiserer oss med har løst disse utfordringene.

I kapittel 5 ser jeg først i punkt 5.1 på bakgrunnsretten i Norge. Denne er viktig for forståelsen rundt problemene inkorporering av straffeansvar for forberedelseshandlinger kan medføre. Jeg ser deretter på hensynene som gjør seg gjeldende for og mot en slik innføring av straffeansvar. I punkt 5.3 ser jeg på likhetene mellom datakriminalitet og andre rettsfelt hvor hovedregelen om straffri forberedelse er fraveket.

Kapittel 6 omhandler art 6 i konvensjonen, og hvorvidt Norge bør inkorporere hele denne i norsk rett. Jeg ser senere på hvordan dette kan manifestere seg i lovverket. Denne problemstillingen tas et skritt videre i kapittel 7, nemlig hvorvidt det kan være fruktbart å ha en mer generell og fleksibel regel rundt dette ansvaret. Jeg ser også på hvordan dette i tilfelle kunne manifestere seg.

Til sist kommer et eget forslag om gjennomføring av forberedelsesansvaret innen datakriminalitet i norsk rett. Forslaget er ikke helt nyskapende, men en videreføring av andre forslag som er lagt frem av andre aktører. Formålet med dette forslaget er å vise at man kan utforme regelen meget omfattende, men likevel ivareta hensynet til legalitetsprinsippet. Fleksibilitet og utvikling trenger ikke stå som et mothensyn til oversiktlighet og forutberegnlighet.

3 HVA ER GJELDENDE RETT OM DATAKRIMINALITET I DAG?

3.1 Gjeldende bestemmelser om datakriminalitet

Det finnes ikke noe eget kapittel i straffeloven av 1902 om datakriminalitet. Dette skyldes den åpenbare årsaken at dette er handlinger som er utviklet den siste tiden. Norske bestemmelser om datakriminalitet er derfor spredt rundt i lovgivningen.

Disse bestemmelsene måtte gjennomgås i forbindelse med vedtakelsen av Europarådets konvensjon om bekjempelsen av datakriminalitet. Konvensjonens bestemmelser måtte inkorporeres i norsk rett. Dette er gjort gjennom endringer og tolkninger av de norske bestemmelsene.

Noen bestemmelser ble forutsatt å dekke konvensjonens krav. Dette omfatter blant annet § 262, som rammer den som ved bruk av en dekodingsinnretning skaffer seg eller annen uautorisert tilgang til en vernet tjeneste. § 151b rammer den som forstyrrer offentlig kringkasting, energiforsyning, elektronisk kommunikasjon og på denne måten volder forstyrrelser i den offentlige forvaltning eller samfunnet for øvrig. §§ 291 og 292, om skadeverk på en løsøregjenstand er forutsatt anvendelighet også på data som endres, slettes eller ødelegges. Selv om det i NOU 1985:35 ble slått fast at data ikke er en materiell løsøregjenstand, ble det forutsatt under vedtakelsen av konvensjonen at denne var dekkende for formålet. Det ble pekt på at lagringsmediet ble forandret når dataene ble det, slik at den mistet sitt formål. § 317 om heleri har vært tolket til også å dekke noen datakriminelle handlinger, som medvirkning til en slik handling. Åndsverkloven § 54a kan ha direkte relevans.

§ 145 ble tilpasset ratifikasjonen av bestemmelsen, og lyder i dag slik:
§ 145 annet ledd lyder i dag slik:

”*det samme gjelder den som uberettiget skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler”*

§ 145 b lyder slik:
”*Den som uberettiget gjør tilgjengelig for andre passord eller andre data som kan gi tilgang til et datasystem, straffes for spredning av tilgangsdata med bøter eller fengsel inntil 6 måneder eller begge deler.*
Grov spredning av tilgangsdata straffes med fengsel inntil 2 år. Ved avgjørelsen av om spredningen er grov, skal det særlig legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen for øvrig skaper fare for betydelig skade”

3.2 Hvor langt strekker ansvaret for forberedelse seg innen datakriminalitet i dag?

Det er sterk norsk rett at man ikke kan straffes for en forbrytelse før den er kommet minst til forsøkstadiet. Dette betyr at ingen kan straffes før man i det minste har passert forsøksgrensen, som er en påbegynnelse på den straffbare handling.
Det finnes noen unntak til denne hovedregelen, der forebygging er særlig nødvendig. Men når det gjelder datakriminalitet er ikke dette vurdert som et slikt område i norsk rett.

Konvensjonen om datakriminalitet inneholder i art 6 regler av forberedende karakter. Denne lyder:
Misbruk av innretninger og tilgangsdata

1. *Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå følgende forsettlige og urettmessige handlinger som straffbare handlinger etter nasjonal rett:*
    a. *Produksjon, salg, erverv for bruk, import, distribusjon eller tilgjengeliggjøring på annen måte av:*
        i. *En innretning, herunder et dataprogram, utviklet eller tilpasset hovedsakelig i den hensikt å begå en av de straffbare handlingene fastslått i samsvar med artikkel 2 til 5,*
        ii. *Et passord, adgangskode eller lignede data som gir tilgang til hele eller deler av et datasystem,*
    b. *Besittelse av utstyr og adgangskoder omhandlet i bokstav a) i) eller ii) ovenfor i den hensikt å bruke det for å begå de straffbare handlingene fastslått i artikkel 2 til 5. En part kan i sin nasjonale rett stille vilkår om besittelse av slikt utstyr eller slike adgangskoder i et visst omfang før det får strafferettslige følger.*
2. *Denne artikkel skal ikke tolkes slik at produksjon, salg, erverv for bruk, import, distribusjon eller tilgjengeliggjøring på annen måte eller besittelse omhandlet i nr 1 i denne artikkel medfører strafferettslig ansvar når det ikke skjer i den hensikt å begå en straffbar handling fastslått i samsvar med artikkel 2 til 5 i denne konvensjon, som autorisert testing og beskyttelse av et datasystem.*
3. *Hver part kan forbeholde seg retten til ikke å anvende nr 1 i denne artikkel, forutsatt at forbeholdet ikke gjelder salg, distribusjon eller tilgjengeliggjøring på annen måte av utstyret og adgangskodene omhandlet i nr 1 bokstav a) ii*[21]*).*

Det er altså i punkt 3 gitt statene en mulighet til å reservere seg mot deler av denne. Det konvensjonen ikke lar statene reservere seg mot, som er obligatorisk for alle statene å ha regler om, er:

[21] Oversettelse fra Ot. Prp. Nr. 40 (2004 – 2005)

Salg, distribusjon eller annen tilgjengeliggjøring på annen måte av midlene som er nevnt i bokstav a) ii), som er passord, adgangskode eller lignende data som gir tilgang til hele eller deler av et datasystem. Med andre ord forskjellige former for spredning av disse kodene.

Denne bestemmelsen banet vei for endringene og gjennomføringen av § 145 b, om spredning av tilgangsdata, og denne dekker i dag den delen av bestemmelsen hvor det ikke var adgang til reservasjon. Norge valgte å reservere seg mot en videre kriminalisering av forberedelseshandlinger. Ansvaret strekker seg derfor til og med § 145 b.

Når det gjelder befatningsformene "salg, distribusjon eller tilgjengeliggjøring på annen måte" kan dette sammenfattes i ordet spredning. Ordene "tilgjengeliggjøring for andre" ble ansett for å være dekkende etter norsk rett, fordi man ved brudd på denne straffes for spredning. I tillegg må befatningen være uberettiget. Når det gjelder det objektive gjerningsinnholdet ble det ansett tilstrekkelig å nevne "passord eller andre data som kan gi tilgang til et datasystem". Dette straffes altså som spredning av slike midler, som en selvstendig straffbar handling. Punkt 2 i konvensjonen presiserer at dette kun skal være ulovlig der det foreligger en hensikt om å begå en av nærmere definerte straffbare handlinger. Etter norsk gjelder alminnelig forsett om befatningen, samt at handlingen i seg selv er straffbar. Dette medfører at forsøk på å bryte straffebudet er straffbart etter § 49.

3.3 Hvilke endringer er gjort de siste årene?

Justisdepartementet ba i 1982 Straffelovrådet om en utredning om datakriminalitet, hvilke regler som fantes på tidspunktet og hva som burde endres. Dette rådet ble ledet av Johs. Andenæs, og resulterte i NOU 1985:31. Denne utredningen introduserte tanken om at data ikke er en gjenstand, men noe av immateriell art. Man kan altså ikke anvende tyveriparagrafen på denne typen informasjon, fordi den ikke er håndfast i sin form. De mente også at forstyrrelsen av en informasjonsstrøm ikke kan rammes av bestemmelsen om skadeverk.

De foreslo endringer eller tilføyelser til §§ 145, annet ledd, 151b, 261, 270 nr 2 og 403.

Denne utredningen ledet til Ot.Prp nr 35. Og med noen få endringer, og med unntak av § 403 ble disse endringene gjennomført ved lov av 12 juni 1987 nr 54. § 145 annet ledd ble opphevet og det ble tilføyd et nytt; ”*det samme gjelder den som ved å bryte en beskyttelse eller på lignede måte skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler”.*

§ 262 ble tilføyd i 1995, og rammer nedtaking av fjernsyns- og radiosignaler ved bruk av piratdekoderfiltre. Denne ble igjen endret i 2001 til sin nåværende form.

I 2002 kom delutredning VII fra straffelovutvalget om ny straffelov, NOU 2002:4. Denne inneholder en del generelle tanker og prinsipielle synspunkter om kriminalisering og behovene for dette, som skulle legges til grunn ved arbeidet med den alminnelige delen i straffeloven. Denne introduserte tanken om å ha alle regler angående datakriminalitet i et eget kapittel, kap 23, kalt ”*vern om informasjon og informasjonsutvikling*”.

I 2003 kom lov om elektronisk kommunikasjon nr 83. Denne inneholder en del legaldefinisjoner av ord som ”bruker” og ”elektronisk kommunikasjon”. Den inneholder noen regler om å gi forskift om plikt til å lagre trafikkdata i en bestemt periode. En slik plikt må forelegges Stortinget for godkjennelse, men er omdiskutert i dag både nasjonalt og internasjonalt.

I Budapest 23 november 2001 undertegnet Norge Europarådets Konvensjon om datakriminalitet. 11 januar 2002 ble datakrimutvalget oppnevnt. Dets oppgave var å gjennomgå hvilke endringer som hadde skjedd siden 1985. Utvalget skulle også se på hvilke endringer som var påkrevd eller ønskelige for at Norge skulle kunne ratifisere Europarådets Konvensjon av 2001. På de punktene hvor konvensjonen åpner for at statene kan reservere seg skulle konvensjonen også gjennomgå om dette burde gjøres. I tillegg

skulle de se spesielt på om det var behov for lovendringer for å styrke vernet mot terrorangrep på datasystemer, og om det burde innføres en loggføringsplikt for trafikkdata.

Datakrimutvalget foreslo å endre § 145 annet ledd og § 145 b til å lyde slik den lyder i dag. Dette dekker den delen av art 6 som statene ikke kunne reservere seg mot. De gikk altså inn for kun å implementere de delene som var påkrevet. De mente at Norge burde benytte den reservasjonsadgangen som forelå. De henviste til neste delutredning for videre behandling av dette spørsmålet, altså den delutredningen som kom i 2007.

Etter dette ble utredningen sendt på høring til en rekke innstanser. Justisdepartementet fremmet 17 desember forslag om samtykke til ratifikasjon av konvensjonen, med de endringene som ble foreslått i NOU 2003:27.

Men de foreslo en annen inkorporering av art 6, og ønsket å omfatte større deler av denne. Denne ble foreslått å lyde slik:

”*den som uberettiget fremstiller, anskaffer, besitter eller gjør tilgjenglig for andre*

a) passord eller andre data som kan gi tilgang til et datasystem, eller

b) dataprogrammer eller andre innretninger som er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer straffes med bøter eller fengsel inntil 6 måneder eller begge deler”

De ønsker altså å kriminalisere også besittelse, samt å ramme dataprogrammer og andre innretninger i tillegg til passordene og adgangkodene. De fleste høringsinstansene uttrykket et ønske om å fjerne kravet om beskyttelsesbrudd, da dette ble for strengt. De legger vekt på at kravet om forsett betyr at de brukere som uskyldig kommer inn på data de skjønner at de ikke har berettiget tilgang til vil tre tilbake og ikke lagre disse. Flere sammenligner og henviser til bestemmelsene om tyveri, som ikke stiller noe krav til spesielle sikringstiltak. Justisdepartementet legger dette spørsmålet tilbake på datakrimutvalget, men går inn for at det kan innebære en straffeskjerpelse. De nevner problemet med identitetstyveri som

eksempel på hvorfor det er viktig med et sikkert vern av data. Likevel tar de ikke ytterligere stilling til spørsmålet, men henviser til at det trenger ytterligere utredning.

I Ot.Prp nr 40 ble dette ikke fulgt opp, da man mente at det holdt med å vente med dette til den andre delutredningen fra datakrimutvalget kom senere. Det ble derimot lagt opp til en bruk av en rettsstridsreservasjon, for å sile ut de tilfellene der adgangen er legitim. Det er altså kun uberettiget tilgang som skal straffes.

I innst.O nr 53 ble den ordlyden som vi har i dag, og som datakrimutvalget også gikk inn for, forseslått. Den ble senere vedtatt i Stortinget. Når det gjelder art 6 og reservasjonsadgangen henviser de til datakrimutvalgets utredning. De nevner kort to delte syn som har kommet frem fra høringsinstansene, men konkluderer etter et sitat av Andenæs ”*gjerningsmannens opptreden må vise at nå er forberedelsens og overveielsens tid forbi, nå skrider han til verket”* Dette er Andenæs' definisjon av grensen mellom forberedelse og forsøk, og er for øvrig ikke særlig informativ for hva som er vektlagt som grunn til å benytte reservasjonsadgangen.

Beskyttelsesvilkåret er fjernet, slik at bestemmelsen er endret fra en beskyttelsesbruddbestemmelse til en datavernbestemmelse, ”*beskyttelsesbrudd, skadeforvoldelse eller vinnings hensikt bør være straffeskjerpende omstendigheter*”.

Mindretallet foreslo at vi skulle kriminalisere også besittelse og spredning av hackerverktøy og passord, slik departementet gikk inn for. De begrunnet dette med at slik rettstilstanden er i dag er derfor ikke straffbart å gjøre slike innretninger tilgjengelig for andre, selv om man med sikkerhet kan si at de vil bli brukt til straffbare handlinger.

Den 4 mars 2005 ble denne ordlyden vedtatt:
§ 145 annet ledd:

”*det samme gjelder den som uberettiget skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler”*

§ 145 b:
”*Den som uberettiget gjør tilgjengelig for andre passord eller andre data som kan gi tilgang til et datasystem, straffes for spredning av tilgangsdata med bøter eller fengsel inntil 6 måneder eller begge deler.*
Grov spredning av tilgangsdata straffes med fengsel inntil 2 år. Ved avgjørelsen av om spredningen er grov, skal det særlig legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen for øvrig skaper fare for betydelig skade”

Ved kgl.res av 4 november 2005 ble ratifikasjon av Europarådets Konvensjon om Cybercrime vedtatt og gjennomført ved endringslov av 8. april 2005 nr 16.

Når det gjelder ansvaret for forberedende handlinger har denne tydelig blitt utvidet de siste årene. Først og fremst med ratifikasjonen av konvensjonen om datakriminalitet og dens art 6, som har ledet til § 145 første, annet ledd og litra b, samt §§ 317 og 262.
Denne gjelder nettopp handlinger som er nødvendige forberedende handlinger til de handlingene som er listet opp i konvensjonens art 2-5, eller dekket gjennom norsk rett av andre paragrafer. For å bryte art 2-5 er det ofte et nødvendig skritt først å bryte art 6. Denne artikkelens funksjon er derfor mye å representere en mulighet til å gripe inn tidligere i begivenhetene.

3.4 Hva er foreslått av videre endringer innenfor datakriminalitet?

Datakrimutvalget kom med den andre delutredningen, NOU 2007:2. Her tar de opp de problemstillinger som fortsatt står på trappene i forbindelse med arbeidet med den nye straffelovens spesielle del. Mens den første delutredningen befattet seg med de endringer

som måtte til for å kunne ratifisere konvensjonen, befatter denne seg med hvilke endringer som fortsatt er ønskelige, etter at litt mer tid har passert.

De foreslår for det første å samle alle datakriminalitetshandlinger i ett kapittel, og vil kalle det "*vern av data, databasert informasjon og datasystemer*". Det er viktig å ha reglene om datakriminalitet i et eget kapittel for å unngå uoversiktlighet og tvilsomme tolkninger av forskjellig andre straffebud.

Lovutkastet inneholder en del paragrafer som på forskjellig måte og i forskjellig omfang dekker konvensjonens krav. Den starter på samme måte som konvensjonen med en liste med definisjoner.

§ 1 – definisjoner

I § 1 foreslår utvalget å ta inn en del definisjoner. De ønsker å definere ordene data, datasystem, dataprogram, databasert informasjon og elektronisk kommunikasjonsnett. Det er ikke noen tradisjon for slikt oppsett i norske lover. Selv om konvensjonen selv bruker dette oppsettet er det ikke særlig heldig i den norske loven. Det er mer naturlig å innta slike definisjoner i særlovgivningen. Eller som Schjølberg foreslår; å innta de i Lov om Elektronisk Kommunikasjon, av 4.7.2003 nr 83[22].

Art 2-5 i konvensjonen må dekkes av norsk rett, og inkorporeres i det nye kapittelet. Dette foreslår utvalget å løse med disse paragrafene:

§ 4 – ulovlig tilgang til datasystem

Denne dekker det samme gjerningsinnholdet som art 2 i konvensjonen.

§ 5 – informasjonstyveri

§ 6 – datatyveri

[22] høringsuttalelse til NOU 2007:2 s 9

§ 9 – etterfølgende befatning med data

Disse dekker gjerningsinnholdet i art 3 i konvensjonen. Hvorfor utvalget velger å skille mellom datatyveri og informasjonstyveri er vanskelig å si. Dette fremstår som samme gjerningsinnhold. § 9 om etterfølgende befatning med data kan også dekke art 4 dersom dataene endres. Hvorfor art 4 da deles inn i §7 om datamodifikasjon og denne § 9 er usikkert.

§ 7 – datamodifikasjon

Denne dekker gjerningsinnholdet i art 4.

§ 8 – uberettiget bruk av datasystem

§ 13 – driftshindring

Disse dekker gjerningsinnholdet i art 5, men hvorfor den er delt inn i driftshindring og uberettiget bruk er også usikkert. Samtidig kunne paragrafen om uberettiget bruk og den om etterfølgende befatning kanskje slås sammen.

Etter denne gjennomgangen av konvensjonens system har utvalgets forslag enda noen bestemmelser som synes å komme i tillegg. Dette er § 2, § 14 og § 15 og § 16.

§§ 2, 14, 15 og 16 gjør noen forberedelseshandlinger som før har vært straffrie frem til de manifesterer seg i en straffbar handling til selvstendige straffebud.

§ 14 – masseutsendelse av elektroniske meldinger

§ 15 – identitetstyveri og bruk av uriktig identitet

§ 16 – kontomisbruk

§ 2 – elektronisk kartlegging

Det er ikke spesielt begrunnet i utredningen hvorfor disse handlingene er spesifisert på denne måten. For å opprettholde den teknologiske nøytralitet og oversiktlighet burde denne bestemmelsen heller være inntatt i særlovgivningen, evt i kombinasjon med en mer generell

regel om forberedelse til straffbare handlinger i straffeloven. Schjølberg mener at også denne kunne høre hjemme i Lov om Elektronisk Kommunikasjon, som §1.

Når det gjelder konvensjonens art 6 om forberedelseshandlinger er den ikke særlig spesifikk eller dekkende. Den går ikke spesielt inn på problemstillingene som denne reiser. Den foreslår isteden å dekke denne artikkelen delvis og oppstykket med §§ 3, 10, 11 og 12. Disse dekker da forskjellige befatningsformer med innretninger og utstyr (§ 3, 11 og 12) samt ulovlige befatningsformer med tilgangsdata (§ 10).

§ 3 – ulovlig anbringelse av utstyr
§ 11 – skadelig dataprogram og utstyr
§ 12 – spredning av selvspredende programmer

Disse omhandler det som art 6 a i) også rammer, befatninger med innretninger og programmer. Befatningsformen ”*anbringelse*” synes å ramme det å sette opp, eller rigge opp, utstyr som er egnet til å få tilgang til informasjon. Dette gjelder utstyr som er særlig egnet til å bryte §§ 5,6 eller 10, altså informasjonstyveri, datatyveri eller ulovlig befatning med tilgangsdata. Man kan spørre seg hvorfor de ikke har valgt en mer åpen form her, slik at bestemmelsen kan ramme brudd på andre straffebud også. De skadelige dataprogrammene og utstyret som nevnes i § 11 er slike som er særlig egnede til å bryte §§ 4-8, 10, 13, 14. Dette gjelder i grunnen alle de handlinger som ikke er av mer spesiell art, som § 2. Nesten alle tenkelige befatningsformer nevnes. § 12 gjelder spredning, men kun av selvspredende programmer. Man må ha kunnskap om at programmene er selvspredende. Det at man mister kontrollen på omfanget av skadene gjør dette til en farlig handling. Likevel er det underlig at dette er en egen bestemmelse, ettersom spredning av tilgangsdata i seg selv er straffbart. Det er spredningen som gjør dette straffbart, fordi man da mister kontrollen over den videre spredingen av programmene. Selv om selvspredende programmer med større visshet vil spres er det allerede vurdert dit hen at alminnelig forsett om spredning er tilstrekkelig.

§ 10 – ulovlig befatning med tilgangsdata

Denne omhandler art 6a ii)

Denne ramser opp alle befatningsformene. Kriteriet er at befatningen er urettmessig.

Utvalget synes å bygge kapittelet opp på en meget detaljbasert måte. Den foreslår å kriminalisere de forskjellige handlinger som omfattes av konvensjonen, men ikke på en direkte måte. Den deler disse opp og sprer dem over flere bestemmelser, som ikke virker mer oversiktlig enn det oppsettet som benyttes i konvensjonen. I tillegg er det lagt til enkelte handlinger, som § 9 om etterfølgende befatning med tilgangsdata. Dette fremstår som overflødig, ettersom dette konsumeres allerede av § 7.

Forslaget favner vidt og omfatter det meste, men synes å feile i å fange den utvikling som fortsatt forutsettes å finne sted. Det kan virke som den har kartlagt hvilke kriminelle handlinger som er en utfordring i dag, og prøver å ramme disse i størst mulig grad. Det blir derimot et klønete oppsett, med mye overlapping og gjentakelse. Samtidig klarer den ikke å rette seg mot det som nettopp er typisk for denne typen kriminalitet, nemlig den raske utviklingen og den store kreativiteten ved påfunn og gjennomføring av nye forbrytelser. Den baserer seg på et prinsipp om teknologinøytralitet slik at den skal imøtekomme utviklingen, men med sine spesielt og snevert utformede straffebud feiler den i nettopp dette.

I denne oppgaven er det forberedelseshandlinger som skal diskuteres. Det skal derfor ikke gås videre gjennom de andre bestemmelsene i kapittelet om datakriminalitet i straffeloven. Oversikten over viser hvilke bestemmelser som har med art 6 i konvensjonen å gjøre, og hvilke som er lagt til.

3.5 Hvilke regler har vi om forebygging av cyberterrorism, og hvilke endringer står på trappene?

Europarådet vedtok i 1977 "The European Convention on the Suppression of Terrorism"[23]. I tillegg har FN vedtatt en konvensjon i 1999 og en resolusjon i 2001 om blant annet finansiering av terrorisme. Dette internasjonale samarbeidet om bekjempelsen av terror har ført til et behov for å definere uttrykket. Dette samarbeidet har videre ført til den utformingen vi har i norsk rett i dag.

Dagens lovgivning definerer en del alvorlige forbrytelser, som drap og grov frihetsberøvelse, som terrorhandlinger, dersom de er begått med det nødvendige forsett. Den definisjon som er tatt inn i norsk lov av ordet "terrorisme" finnes i straffelovens § 147a og lyder: "*en straffbar handling som nevnt i…"* en rekke andre bestemmelser. Den bestemmelsen som dekker datakriminalitet er § 151 b om "forstyrrelser av informasjonssamling, energiforsyning, kringkasting, telekommunikasjon eller samferdsel". I tillegg må en av disse handlingene være begått med minst ett av disse forsettene:

- å forstyrre alvorlig en funksjon av grunnleggende betydning i samfunnet
- å skape alvorlig frykt i befolkningen
- å tvinge myndighetene til å tåle, gjøre eller unnlate noe av vesentlig betydning for landet, typisk å tvinge myndighetene til å treffe en bestemt avgjørelse.

For å kvalifisere som terrorisme må det altså dreie seg om en av disse opplistede forbrytelsene, og gjerningsmannen må i tillegg oppfylle minst ett av de tre forsettkravene.

I 2005 kom en tilleggsprotokoll til terrorkonvensjonen av 1977, "Council of Europe Convention on the Prevention of Terrorism"[24]. Den trådte i kraft 1 juli 2007. Denne gjelder, i motsetning til bekjempelse av terrorhandlinger, forebygging av slike. Den pålegger statene å kriminalisere trusler om å gjennomføre de hovedhandlingene som er definert som

[23] www.coe.int

[24] se conventions.coe.int, samt vedlegg 2

terrorisme. I tillegg anbefaler den kriminalisering av deltakelse i terrorgrupper, terrorfinansiering og forbund. For forebygging ønskes det kriminalisering av offentlig oppmuntring, verving og opplæring i terrorisme.
Denne konvensjonen er ikke signert av Norge.

Arbeidet med å utrede hvorvidt Norge bør signere og senere ratifisere denne konvensjonen om forebygging av terror er i gang i disse dager. Justisdepartementet foreslår noen endringer, blant annet i § 147a om definisjonen av terrorisme. Denne innebærer en skjerping og presisering av begrepet. Når det gjelder bestemmelsene rundt forberedelse og planlegging av terrorhandlinger er disse ikke foreslått videreført i norsk rett. Det samme gjelder bestemmelsene om å true om å begå en terrorhandling. Det foreslås også å erstatte kravet om terrorforsett med terrorhensikt. Dette forslaget fra justisdepartementet er sendt til høring.

Høringsuttalelsen fra lovavdelingen viser til at det ikke er tradisjon for å kriminalisere slike tidlige handlinger i norsk rett. De mener at medvirningsansvaret går langt nok til å dekke reglene om forebygging av terrorisme, som oppmuntring, verving og opplæring i terrorisme, i samband med § 140 i straffeloven. De foreslår likevel en egen bestemmelse om de tre handlingene med en felles strafferamme på 6 år.

For forberedende handlinger foreslår de å ramme trusler om å begå en terrorhandling med en strafferamme på fengsel inntil 12 år. For deltakelse i terrorgrupper viser lovavdelingen til § 104a om deltakelse i organiserte miljøer, og det faktum at Norge ikke er forpliktet til å medta denne bestemmelsen. De foreslår ikke en videreføring av denne. For finansiering og forbund foreslås en strafferamme på 10 år.

4 FREMMED RETT

4.1 Internasjonal rett

Det er flere internasjonale organisasjoner som jobber med bekjempelsen av cybercrime. FN vedtok i 2005 en etablering av lovgivning og andre tiltak, som ITU har fått i oppgave å gjennomføre. Dette er globale konferanser og tilbud om informasjon og opplæring, hvor de blant annet fokuserer på harmonisering av regelverk mellom landene. Se nærmere om dette på ITU's webside[25]. Europarådet vedtok i 2001 sin konvensjon om bekjempelsen av datakriminalitet. EU har også satt i gang arbeidet med dette, mer informasjon om det kan finnes på deres nettsteder[26].

En rekke andre land i Europa, men også USA, har gjennomført endringer for å møte konvensjonen til Europarådet, eller kun for å møte den generelle utviklingen som skjer innen dette emnet. Jeg skal se litt nærmere på våre naboland, Sverige og Danmark.

4.2 Svensk rett

Svensk rett ble endret i 2001 for å møte utviklingen i dataverden. Prop 2000/01:85 sier mye om hvorfor dette ble ansett som et viktig skritt mot bekjempelsen av datarelatert kriminalitet.
Propposisjonen utreder en del spørsmål om forberedelse til forbrytelser, og foreslår endringer til §§ 7 og 8 i tredje kapittel og til § 2 i tjuetredje kapittel
Dette gjelder blant annet § 2 i kap 23 om "*förberdelse till brott*".

[25] www.itu.int/osg/spu/cybersecurity

[26] www.coe.int

Det ble fremmet forslag om en reform av forberedelsesansvaret. Grunnen er blant annet at den oppregningen som var foretatt i lovteksten var gammeldags, særlig med tanke på IT miljøets utvikling og ny teknologi. Det ble trukket frem at man skulle ramme hjelpemidler som er særskilt egnet som hjelpemiddel til en forbrytelse.
Det ble foreslått heller å bruke betegnelsen ”noe som er særskilt egnet til å anvende som hjelpemiddel til en forbrytelse”. Dette mente de ville kunne dekke også fremtidige hjelpemiddel som man ikke kan forestille seg i dag. De ville dekke befatning med alle gjenstander som ikke har noe annet anvendelsesområde enn å begå forbrytelser. Objektet måtte ha en noenlunde sentral betydning for gjennomføringen av forbrytelsen.

Sverige undertegnet Europarådets konvensjon den 23 nov 2001.

Ôveråklageren, Gunnel Lindberg, fikk i oppdrag fra justisdepartementet å utrede svensk rett og hvorvidt de burde ratifisere Europarådets konvensjon.
Hun gikk inn for ratifisering.

Ettersom svensk rett er et av de systemer som tidlig tok fatt utviklingen som skjer på det kriminelle markedet, og deriblant når det gjelder IT-kriminalitet, foreslås det ikke mange endringer, ettersom den allerede dekker kravene i konvensjonen tilfredsstillende.
Bare art 11 om forsøkstraff kan tenkes å gå videre når det gjelder simple forbrytelser, enn slik det allerede er i svensk rett.

Det fastslås at den endringen som fant sted i svensk rett i 2001 dekker konvensjonens krav om hjelpemidler, altså at den oppregningen som tidligere var brukt ble erstattet med den generelle formuleringen ”noe som er særskilt egnet til å anvende som hjelpemiddel ved en forbrytelse”.
Det nevnes at hvorvidt adgangskoder og passord er slike hjelpemidler, så kan disse nærmest sammenlignes med nøkler. De har jo et legitimt anvendelsesområde, og det kan diskuteres om de er særskilt egnet til brudd. Likevel ble det avgjort i NJA 1960 s 442 at nøkler som ble oppbevart hos en person som ikke var ment å ha adgang til det stedet som

nøklene ga adgang til kunne anses som forberedelse til ulovlig inntreden til dette stedet. Det er jo ikke tvil om at ulovlig inntreden i annens bolig er innbrudd selv om denne hadde nøkler, dersom nøklene er stjålet.
Det bekreftes derfor at ulovlig besittelse av adgangskoder og passord nettopp er særskilt egnet til forbrytelser dersom det er i feil hender, når det gjelder IT og dataverdenen. Kravene i art 6 ble dermed ansett å være oppfylte, Sverige så ingen grunn til å reservere seg.

§ 2 lyder i dag:

”Den som, med uppsåt att utföra eller främja brott, …

… 2. skaffar, tillverkar, lämnar, tar emot, förvarar, transporterar, sammanställer eller tar annan liknande befattning med något som är särskilt ägnat att användas som hjälpmedel vid ett brott,

skall i de fall det särskilt anges dömas för förberedelse till brottet, om han inte gjort sig skyldig till fullbordat brott eller försök.

I de fall det särskilt anges döms för stämpling till brott. Med stämpling förstås, att någon i samråd med annan beslutar gärningen eller att någon söker anstifta annan eller åtar eller erbjuder sig att utföra den.

(*2001:348*).[27]

4.3 **Dansk rett**

Den danske straffelov § 21

”*Handlinger, som sigter til at fremme eller bevirke udførelsen af en forbrydelse, straffes, når denne ikke fullbyrdes, som forsøg.*

Den for lovovertrædelsen foreskrevne straf kan ved forsøg nedsættes, navnlig når forsøget vidner om ringe styrke eller fasthed i det forbryderske forsæt.

[27] Fra rättsnättet – svensk nettside ála lovdata

For så vidt ikke andet er bestemt, straffes forsøg kun, når der for lovovertrædelsen er foreskrevet højere straf end hæfte".

Danskene har definert forsøk mye videre enn mange andre land. De inkluderer det de fleste vil karakterisere som straffri forberedelse innen forsøksbestemmelsen. Denne gjelder alle former for forbrytelser, og enhver forberedelse på denne. Danskene har således allerede her oppfylt konvensjonens art 6 og vel så det. Bestemmelsen favner meget vidt, loven krever faktisk ikke annet en at det foreligger en handling som kan være en forberedelse på en straffbar handling. Der er ingen faste prinsipper om at handlingen må være så eller så klar, at den må manifestere seg utad. Alt er opp til rettspraksis og skjønn.

Det kreves selvfølgelig subjektivt sett forsett om å fullføre forbrytelsen, jf "sikter til".
Det kreves normalt ikke mer enn vanlig forsett, men det er argumentert for at man på tidlige tidspunkt i forberedelsen bør kreve en hensikt, for å stramme inn begrepet noe.
Danskene vedtok i 5.nov. 2005 en lov om bekjempelsen av datakriminalitet og dekker med den de resterende artiklene i konvensjonen.

En dom fra København tingrett[28] er av interesse her. En dansk/marokkaner ble dømt for medvirkning til terrorisme. Han er dømt for å ha oppfordret offentlig til gjennomføringen av terrorhandlinger. I tillegg har han bistått med veiledning på et profesjonelt plan.
Han brukte i stor grad cyberspace som arena for dette. Mannen ble dømt for medvirkning til en straffbar handling. Han misbrukte cyberspace da han ga denne veiledningen, men han ble ikke dømt for noen form for datakriminalitet. Likevel kan dommen illustrere hvordan datasystemer kan misbrukes til slike formål, og hvordan det blir gjort.

[28] dom av 11-04-2007

5 FORBEREDELSE INNEN DATAKRIMINALITET

5.1 Bakgrunnsretten

Etter norsk rett er ikke forberedende handlinger straffbare. Handlinger er ikke straffbare før de har passert det man kaller forsøksgrensen. Denne er definert av Andenæs som at ”*gjerningsmannens opptreden må vise at nå er forberedelsens og overveielsenes tid forbi, nå skrider han til verket*”[29].
På den ene siden er det ikke ønskelig å kriminalisere mer enn hva som er nødvendig i et samfunn. Straff er det strengeste onde staten påfører individene, og er ment å regulere adferd. På den annen side kan utviklingen som finner sted på enkelte områder gjøre det nødvendig å fravike dette prinsippet. Et overordnet hensyn er at Norge bør følge den utvikling som skjer internasjonalt og overholde sine folkerettslige forpliktelser. I forbindelse med arbeidet med den nye straffelovens alminnelige del er det utredet hvorvidt det er på sin plass med en utvidelse av straffeansvaret i norsk rett, altså om forsøksgrensen skulle utvides. Erling Johannes Husabø ble bedt av straffelovkommisjonen å utrede dette spørsmålet. Han spurt om å utrede hvordan rettstilstanden var på dette tidspunktet, i 1999, og hvilke endringer som burde gjøres.

Husabø konkluderte i det store og det hele at det etter hans skjønn ikke var ønskelig med noen utvidelse av det forberedende ansvaret på et generelt grunnlag, men at det kunne være spesielle rettsområder der dette er spesielt nødvendig. Dette begrunnet han med at man frykter en overkriminalisering og en uviss rettstilstand for borgerne, dersom man kriminaliserer for vide områder. Dette ville også prosessmessig føre til en økt kontroll i den private sfære. Han peker på at for å legitimere en slik utvidelse må man i første omgang kunne dokumentere et behov for dette i samfunnet, og at dette ikke er utredet nok slik det er i dag. For det andre må de økonomiske konsekvensene utredes. Han betviler de

[29] Andenæs, Johs. *Alminnelig strafferett* s 347

preventive virkningene en straffbar forberedelseshandling har for borgerne. Han peker på at andre lands erfaringer på området er at slike straffebud blir lite konkrete og tydelige, og at mye blir overlatt til påtalemakten og dommernes skjønn. Han mente at det er nesten umulig å påvise en hensikt eller det nødvendige forsett i slike tilfeller.

Som eksempler på områder hvor det kan tenkes unntak nevner Husabø terrorrelaterte handlinger og andre trusler mot rikets sikkerhet. Felles for disse er at de utgjør en stor trussel for liv og helse, og for Norge som selvstendig stat. Det er mulig at forberedelse til den terrorisme som kan gjennomføres hovedsakelig med bruk av dataprogrammer og Internett er et slikt område som Husabø ville ha kriminalisert. Husabø er altså imot en generell forberedelsesregel som i Danmark, men ikke en mer avgrenset regel som treffer et mindre område. Han går inn for å regulere dette noe mer spesifikt for de spesielle områdene, fordi det blir for omfangsrikt og har for mange uforutsette følger å gjøre dette helt generelt.

5.2 Hensynene for og mot utvidelse av ansvaret

Negative konsekvenser av økt kriminalisering er som Husabø nevner faren for overkriminalisering, økt kontroll i den private sfære og den uvisse rettstilstanden dette kan medføre. Faren for overkriminalisering gjelder for en generell utvidelse av forsøksgrensen, men er ikke spesielt stor om man kun rammer datateknologien. Rettstilstanden vil ikke bli mer uviss dersom reglene som utformes er tilstrekkelig klare og utvetydige. Det er viktig at legalitetshensynet blir ivaretatt her. Jeg minner også om at konvensjonen ber oss kriminalisere spesielle former for uberettiget befatning med passord, og med slikt utstyr som er særlig egnet som hjelpemiddel i en straffbar handling. Det skal således ikke være tvil om hva som rammes. Data som har flere legitime formål skal ikke rammes av ansvaret.

Det er nødvendig å påvise et tilstrekkelig behov i samfunnet før man fraviker en hovedregel. Behovet for å forebygge cybercrime, og i ytterste konsekvens cyberterrorism, kommer frem på mange måter.

Den organiserte kriminaliteten som i øker er et eksempel. Disse bruker i økende grad data som mål, middel og arena for sin virksomhet. Dette gjør de blant annet fordi mulighetene her er mange, det er internasjonalt og oppdagelsesrisikoen er lav.
Økonomisk kriminalitet fra utlandet er vanlig, særlig fra østblokk-land. Det internasjonale nettet gjør verden til en enhet. Land med høyere kriminalitet enn vårt eget får nye arenaer å jobbe på. Norge, som et rikt land, blir et attraktivt offer. Gjerningene påfører samfunnet enorme kostnader og hindrer den ønskelige utviklingen av e-handel. Parallellen til sprengstoff er nærliggende. "Datavirus, hackerverktøy og lignende dataprogrammer kan betraktes som elektronisk sprengstoff[30]".
De som arbeider med dette er profesjonelle kriminelle, og de arbeider med en innsats og en innsikt som er vanskelig å få tilgang til. Hele deres "arbeidsdag" er en forberedelse til kriminelle handlinger. Arbeidsfordelingene mellom de forskjellige partene gjør sjansen for at de planlagte handlingene gjennomføres stor. Det opereres innenfor lukkede miljø, politiet vet ikke hvem som er medlem, hvilke handlinger de forbereder eller hvordan de kan forebygge skadene. Den største faren innenfor slike miljøer er faren for cyberterrorism. Dersom enkelte grupper får tilgang til tilstrekkelig utstyr og kunnskap utgjør dette en stor trussel for samfunnets infrastruktur.
Dette fører til neste argument, om at en utvidelse av politiets kompetanse er en sentral muligheten for å få bukt med dette i større skala. Selv om dette reelt sett fører til en fare for større kontroll i den private sfære vil det også ha tydelige og viktige positive virkninger.

Her kan man trekke en parallell til en annen del av de kriminelle, de mer "hobbybaserte". En del av de kriminelle handlingene blir faktisk gjennomført på gutterommet, av gutter i tenårene[31]. Dette er ikke mennesker som ikke anser seg selv som kriminelle, men heller

[30] ØKOKRIM i høringsuttalelse

[31] mørketallsundersøkelsen 2006 og uttalelse fra politiinspektør Berit Børset Solstad ved Kripos

medlemmer av miljøer hvor det er knyttet status til å inneha den kunnskap og ferdighet som kreves for å bryte beskyttelser og trenge gjennom sikkerhetsnett. Selv om disse ikke utgjør en stor trussel med sin virksomhet viser det seg at de mer hardbarkede kriminelle er interessert i deres kunnskap. Det finnes områder i cyberspace hvor det kjøpes og selges slik kunnskap.

Husabø argumenterer med at den preventive virkningen er lav ved å kriminalisere forberedelseshandlinger, og at de som ønsker å begå slike handlinger ikke blir mer avskrekket fra dette av et forberedelsesdelikt, når ikke hovedstraffebudet gir noen virkning. I de tilfellene som nevnt her tror jeg det kan være omvendt. Disse ”guttene” som utvikler sin kunnskap rundt dette området anser seg ikke som kriminelle, og har antakeligvis ikke noe ønske om å være det heller. I kombinasjon med den lave oppdagelsesrisikoen og fraværet av kunnskap om medvirkningsansvaret tror de faktisk de handler med rette. Dersom omgang med slikt utstyr, eller besittelse av uberettiget tilegnede passord var straffbart i seg selv, ville det kanskje føre til større motforestillinger hos de som handler med dette. At samfunnet tar avstand til slike handlinger øker alvorligheten og moralen rundt handlingene.

Slike handlinger skaper en ”oppsikt og uro” i samfunnet, slik at man bør markere avstand til dem.

Handlinger som innførsel av falske minibankfronter får førstesideoppslag i nyhetene i disse dager. Det strider mot den alminnelige rettsbevissthet at man ikke kan straffe mennesker som innfører slike midler. Det dreier seg om utstyr som ikke har noe annet

For å kunne få utbytte av alle de mulighetene data kan by på er det viktig at det er trygt. Samtidig er det viktig at det er åpent, slik at kriminelle ikke finner fristeder her. Det er viktig at folk har tillit til systemet for at det skal kunne fungere optimalt.

Det er derfor et viktig poeng at ikke en kriminalisering av forberedende handlinger begrenser forskning, utvikling og nyskaptenhet innen feltet. Det skal være rom for eksperimenter, for det er slik utviklingen skjer. Dette er nettopp et område som blir utviklet av mange forskjellige aktører. Internettet, slik vi kjenner det, vil ikke ha stor verdi dersom ikke dette var et hovedprinsipp: at alle fritt skal kunne bruke det og forme det.

Det er derfor spesielt viktig innen dette feltet at straffebudene ikke blir så vide at det fører til en redsel for å utforske feltet. Dette må bæres i minne ved utformingen av straffebudet. Dette er også grunnen til at det i de norske bestemmelsene i dag er lagt til en rettsstridsreservasjon. Denne skal presisere at berettigede handlinger ikke skal anses for straffbare selv om de i prinsippet oppfyller kravene i gjerningsbeskrivelsen. Dette kan ha grunnlag i lov, sedvane eller avtale. Det skal ikke være vanskelig å sile ut de tilfellene der befatningen er rettmessig.

Det kan altså relativt enkelt påvises et behov for økt fokus på cybercrime, både i Norge og internasjonalt.. Til dette argumentet kommer at det er viktig at ikke Norge ender opp med å bli en ”data haven” for de kriminelle, en trygg havn hvor reglene ikke strekker til.

Det viktigste argumentet er derfor at Norge bør følge den utvikling som skjer innen internasjonal bekjempelse av cybercrime. Europarådets konvensjon er ratifisert av 22 stater, deriblant Norge og våre naboland. I hele Europa foregår det for tiden en harmonisering av reglene, slik at samarbeidet skal gå lettere. Land som vi identifiserer oss med har inkorporert art 6 fra konvensjonen i mye større grad enn det Norge har gjort til nå. De har endret eller driver med endringsarbeid for tiden for å følge denne utviklingen. De har i tillegg ratifisert konvensjonen om bekjempelse av terror, som Norge ikke har gjort. Det er viktig, som sagt, at Norge ikke blir hengende etter her, nettopp fordi denne kriminaliteten ikke kjenner noen landegrenser.

5.3 **Datakriminalitet som unntak til hovedregelen**

Spørsmålet er om vi skal kriminalisere flere forberedende handlinger innen datakriminalitet når den nye straffeloven gjennomføres. Forskjellige befatningsformer med data, som er egnet som hjelpemiddel til å begå en annen forbrytelse, er forberedende handlinger. Gjerningsmannen har ikke forsøkt å bruke disse dataene til noe kriminelt, enda, slik at han

fortsatt befinner seg på det straffrie forberedelsesstadiet. Denne befatningen er i seg selv ikke straffbar i dag, så lenge den ikke har resultert i utførelsen av en straffbar handling.

Det er viktig å ha i bakhodet at datakriminalitet dreier seg om immaterielle verdier, som ikke omfattes på en tilfredsstillende måte av det nåværende regelverket. Reglene som hovedsakelig retter seg mot materielle goder kan ikke automatisk få anvendelse på data. Den digitale verden er ikke lik den virtuelle, og byr således på andre utfordringer. Datasystemer verner om interesser av ikke-økonomisk art, som sensitive personopplysninger, og dersom dette skal fungere med tilstrekkelig tillit må det også være konsekvenser for de som bryter denne tilliten. Den tradisjonelle grensen mellom forsøk og forberedelse har gjennomslagskraft når det gjelder fysiske handlinger og materielle goder. Disse er håndfaste og lettere beviselige.

Når det gjelder den digitale verden er forholdene annerledes. For det første kan man ikke med et utrent øye se om en straffbar handling er begått, slik man kan se at noen har brutt seg inn og stjålet verdifull informasjon fra en bolig. Det er derfor både vanskelig å oppdage dette, og å beskytte seg mot det. Mange føler at man må være med i den digitale verden for ikke å være gammeldags og miste forbindelser, samtidig som de kvier seg for den sårbarhet dette innebærer. For det andre er dette et spesielt felt, som ikke angår eller berører mannen i gata i stor grad. Det er ikke nødvendig for noen å omgås passord eller hackerutstyr uten spesiell grunn eller berettigelse, og dette er heller ikke noen beskyttelsesverdig rett. Om ikke det er for å få tilgang til noe uberettiget selv kan det være å videreformidle det til andre mot vederlag.

Utviklingen innen denne teknologien går fortere enn utviklingen innen lovverket. Kreative forbrytelser påviser et behov for å utvide mulighetene til å gripe inn på et tidligere tidspunkt.

Selv om forberedelseshandlinger ikke er straffbare etter norsk rett finnes det som nevnt en rekke unntak til denne regelen. Spørsmålet er derfor hvorvidt datakriminalitet også er et

område som fortjener å bli behandlet som et unntak. Det er et ønske om å ramme slike handlinger fordi de er vurdert som spesielt farlige, uønskede eller spesielle. Et fellestrekk er at nærheten til den faktiske forbrytelsen er stor. I tillegg er det vurdert slik at medvirkningsansvaret ikke strekker til. Dette er tilfellet for avtaler om å begå forbrytelser. Formålet med reglene om avtale er nettopp å treffe de tilfellene som ikke kommer så langt som til forsøk eller fullføring. Å kriminalisere forberedelse her har også sammenheng med at oppdagelsesrisikoen er lav, slik at medvirkere sjelden blir holdt ansvarlig. De forberedelseshandlingene som allerede er kriminaliserte er i forarbeidene til straffeloven begrunnet med at den forbryterske vilje har manifestert seg på en slik måte at "*der lader antage, at den besidder den til Forbrydelsens Udførelse fornødne Styrke og Bestemthed*". Dette er den mer subjektive vurderingen, hvor ønsket om å straffe den forbryterske vilje står sentralt. Noen forbrytelser er så alvorlige og samfunnskadelige at vi kriminaliserer tidligere stadier av slike handlinger. Prinsippet om at man ikke skal straffe noen før de virkelig har utvist den forbryterske vilje får mindre vekt i slike sammenhenger. Selv om man er prinsippfast og mener at man ikke skal straffe mennesker før de faktisk har oversteget grensen for det akseptable hender det at denne grensen blir mindre skarp enn vanlig. Den enkeltes frie tanke blir ikke respektert i like høy grad der gjerningsmannen balanserer på grensen for det straffbare.

De forberedelsesreglene som allerede er rammet i straffeloven er bygget opp på forskjellige måter, og kan tjene som eksempler på hvordan dette kan gjennomføres i praksis innen cybercrime.

Formelle forberedelsesdelikter er de som retter seg mot å forberede en forbrytelse nevnt i et annet straffebud. Et eksempel på dette er § 159 som gjør det til en selvstendig forbrytelse å gjøre forbund om å utføre en rekke nevnte forbrytelser. Skyldkravet er her det sentrale. Dette er samme oppsettet som konvensjonens art 6 legger opp til, nemlig å nevne forberedelseshandlinger til å bryte art 2-5. Man kan også ta referansen til hovedforbrytelsen inn i gjerningsbeskrivelsen, som i § 160, hvor det gjøres til en selvstendig forbrytelse å gi veiledning i bruk av sprengstoff eller gift som en ment til

forøvelse av forbrytelser. Som en tredje variant kan både gjerningsbeskrivelsen og skyldkravet være med, som i § 177. Der kreves det både at redskapene ble anskaffet til forberedelse av en forbrytelse og at redskapene tilkjennegir seg som bestemte til forbrytelsen.

Når det gjelder å utvide straffeansvaret innen cybercrime kan alle disse tre måtene å gjøre det på være aktuelle. Dette kommer jeg inn på i diskusjonen nedenfor om hvordan en slik utvidelse bør manifestere seg. De forberedelsesdeliktene som rammes av konvensjonens art 6 er typiske materielle forberedelsesdelikter, hvor den fysiske befatningen med innretninger eller passord er det sentrale.

6 KONVENSJONENS ART 6

6.1 Bør resten av art 6 inkorporeres i norsk rett?

Når vi nå har sett på behovet samfunnet har for en økt kontroll innenfor dette område, og den utvikling som har skjedd de siste årene, skal vi se litt på andre lovtekniske konsekvenser ved innføringen av art 6 i sin helhet, og hvordan en slik regel kan manifestere seg i norsk rett. Det er bred enighet i alle utredninger om at man bør samle bestemmelsene om datakriminalitet i et eget kapittel, og ikke ha de spredt rundt i lovverket slik det er i dag. Det er altså ingen tvil om at dette er av økende relevans, og skiller seg såpass fra andre former for kriminalitet at det fortjener et eget avsnitt.

Når det gjelder de forberedende handlingene, art 6 i konvensjonen, er dette dekket i norsk rett gjennom de endringer som ble gjort av § 145b. Denne dekker som tidligere nevnt kun den delen av art 6 som det ikke var mulig å reservere seg imot. Utformingen av § 145b skiller seg noe fra den konvensjonen bruker i art 6. Den bestemmer at spredning av passord og andre data som er tilegnet uberettiget skal straffes som en selvstendig handling. Konvensjonen kriminaliserer derimot slike handlinger der dette er en forberedelse på brudd på andre bestemmelser. Det er i konvensjonen ikke bare spredningen i seg selv som er det straffverdige, men der dette gjøres i den hensikt å begå en annen, nærmere definert, straffbar handling. På denne måten rekker § 145b lenger, ettersom det ikke er noe krav at hensikten skal være videre straffbar handling.

Den delen av art 6 som ikke allerede er inkorporert i norsk rett er oversiktlig gjengitt her.

For det objektive gjerningsinnholdet *"passord og adgangskoder*" er befatningsformen tilgjengeliggjøring, eller spredning, kriminalisert. Det som ikke er kriminalisert er

- "*besittelse*" (punkt b)

- fremstilling eller anskaffelse, som konsumerer ordene ”*import*”, ”*produksjon*” og ”*erverv for bruk*”.

For gjerningsinnholdet ”*en innretning, herunder et dataprogram*”, er ikke omfattet i lovverket i dag. Dette vil si hackerverktøy, datavirus av forskjellige slag, altså tekniske hjelpemidler til å begå en av de straffbare handlingene i art 2-5. Ingen form for befatning med slikt utstyr er kriminalisert, verken

- ”*besittelse*” (punkt b)
- ”*tilgjengeliggjøring på annen måte*”, dvs spredning, som konsumerer ordet ”*salg*” og ”*distribusjon”*
- fremstilling eller anskaffelse, som konsumerer ordene ”*import*”, ”*produksjon*” og ”*erverv for bruk*”.

Konvensjonen nevner mange former for befatning som den ønsker å kriminalisere. Mange av disse overlapper hverandre. Det kan argumenteres med at flere befatningsformer listet opp på denne måten gjør bestemmelsen mer stivbent og uoversiktlig. Listen blir for det første lang. For det andre kan det tenkes befatningsformer som ikke rammes her, men som absolutt burde omfattes av reglene. Dette er grunnen til at jeg har sammenfattet disse noe, slik det kommer frem i oversikten over.

Det er allerede vedtatt og godkjent at ordene ”gjør tilgjengelig for andre”, som brukt i § 145b, dekker ordene ”salg, distribusjon og tilgjengeliggjøring på annen måte” som brukes i art 6. Ellers hadde ikke § 145b dekket den delen som konvensjonen påbyr statene å dekke. Det dreier seg kort og godt om spredning. På samme måte kan derfor ordene ”fremstilling og anskaffelse” dekke ordene ”import, produksjon og erverv for bruk”. Diskusjonen dreier seg således om spredning av innretninger og utstyr, besittelse, fremstilling og anskaffelse av passord og innretninger bør være straffbart.

Datakrimutvalget går ikke inn for å kriminalisere besittelse. De henviser til at besittelse ikke isolert sett krenker noen beskyttelsesverdige interesser. De ser likevel risikoen for spredning som en følge av besittelse. Men de mener at selv om denne spredningen også kan skje uten viten og mening utgjør den det neste ledd i den straffbare handling. Først ved spredning har man krenket noen beskyttelsesverdige interesser, ikke allerede ved besittelsen. De viser til at selv om det er straffebelagt å besitte sprengstoff og uran, er det ikke straffebelagt å besitte skytevåpen dersom dette er gjort på lovlig måte, selv om formålet er å ta noen av dage. Selve besittelsen krenker ikke noen på den måten som besittelse av barnepornografi gjør. De går likevel inn for at utredning om besittelse av hackerverktøy og datavirus bør fortsette i neste delutredning.

Justisdepartementet forslår å ramme fremtille, anskaffe, besitte eller gjøre tilgjengelig for andre. Dette er i samsvar med konvensjonen. De nevner det faktum at konvensjonens befatningsformer overlapper hverandre, og sammenfatter dem derfor i disse fire variantene. Når det gjelder besittelse ser de den argumentasjonen som datakrimutvalget står for, nemlig at å kriminalisere dette kan fortone seg som straff for ugjort handling. Men de henviser til det skillet i den psykologiske barriere som finnes når det gjelder datakriminalitet i forhold til annen kriminalitet. De mener at slik kriminalitet ikke virker like avskrekkende som annen kriminalitet, i sammenheng med at mange ikke vet at slike handlinger er kriminelle. Dette bør etter deres mening klargjøres og kriminaliseres. Departementet går med bakgrunn i det store skadepotensialet, hensynet til tilliten til elektronisk kommunikasjon og den lave oppdagelsesrisikoen inn for at det bør være straffbart å besitte hackerverktøy. Dette vil lette arbeidet med å forebygge slik kriminalitet.

Justiskomiteen var mot kriminalisering av besittelse, og dermed enige med datakrimutvalget angående dette. Mindretallet, medlemmene fra Høyre og Krf, mente likevel at vi skulle kriminalisere også besittelse av passord og hackerverktøy, samt spredning av disse. De viste til den begrensede lovlige bruken av slikt utstyr, samt det store skadepotensialet dersom det ble brukt til straffbare handlinger.

Jeg er enig med mindretallet og justisdepartementet her. Besittelse er ingen beskyttelsesverdig interesse i slike tilfeller, ingen trenger å ha krav på å kunne besitte farlige gjenstander med stort skadepotensial. Jeg viser også i den sammenheng til folks tillit til rettshåndhevingen, og den oppsikt slike handlinger medfører. Jeg synes derfor vi også skal ramme besittelse av slikt utstyr som nevnt i konvensjonen. Det er et viktig poeng at disse forberedende handlingene ikke er beskyttet fordi de ikke har noe legitimt formål. Å sitte på adgangskoder og passord, eller data i et datasystem, som man ikke i utgangspunktet har tilgang til kan sammenlignes med å sitte på tjuvegods. Dette er ikke en beskyttet rett, selv om det kan være vanskelig å bevise at det er besitteren som har skaffet kodene på en urettmessig måte. Det eksempelet som ble brukt av datakrimutvalget i deres andre delutredning om elektronisk kartlegging er godt. De begrunner dette nettopp med at slik kartlegging ikke har noe legitimt formål dersom den er uautorisert. Formålet er nettopp å avdekke svakheter, og dette kan gjøres enten i den hensikt å reparere svakhetene eller for å utnytte dem. Dersom kartleggingen er uautorisert er det altså ingen legitim grunn til å foreta den. Det samme gjelder for besittelse av passord og data som er anskaffet på en uberettiget måte.

§ 145 b i straffeloven rammer spredning av tilgangsdata. Denne gjelder passord eller andre data som kan gi tilgang til et datasystem. Når det gjelder spredning av hackerverktøy og andre dataprogrammer med skadevoldende egenskaper, og liten egenverdi, har vi i dag ingen regler.

Datakrimutvalget vil ikke kriminalisere spredning av slikt utstyr. De mener at spredning nettopp er en slik handling som kan rammes av reglene om medvirkning og forsøk. De argumenterer med at den faren som kan oppstå for at noen vil misbruke en innretning eller et program, ikke kan rettferdiggjøre å straffe den som sprer det. Dette begrunner de videre med at en slik person ikke oppfyller skyldkravet, som de mente burde være hensikt. Slike straffebud har vi bare når liv og helse står på spill, som ved knivforbud, farts- og promillebestemmelser. Dessuten vil man ha en hovedmann man kan holde ansvarlig

dersom det først blir begått en kriminell handling. Utvalget går derfor inn for reservasjon også på dette punktet.

Justisdepartementet går derimot inn for at spredning burde være straffbart. De peker på at slike innretninger ikke har noe lovlig formål. Disse er skadevoldende, og selv om man ikke selv vil bruke dem til å begå straffbare handlinger, kan man si det som sikkert at andre vil gjøre det, dersom man gjør det mulig. Det er også et marked her for de organiserte kriminelle. De kan få tak i utstyr gjennom "uskyldige" tredjeparter, som de betaler godt for sine varer. Ettersom disse tredjepartene ikke risikerer noen straff selv utvikler slike innretninger seg lett til en handelsvare. Det finnes i dag flere nettsteder som tilbyr slike programmer mot betaling. Det er helt sikkert at de som kjøper programmene ikke har noe legitimt formål med kjøpet. Likevel kan man i dag ikke straffes for å tilby programmene til andre, ettersom man selv ikke bryter noen straffebestemmelser. Dersom denne spredningen er av stort omfang, og skjer hovedsakelig til en person eller gruppe som kan holdes ansvarlig for å misbruke dem, kan sprederen rammes av medvirkningsansvaret. Medvirkningsansvaret går langt etter norsk rett. Det er ikke aksessorisk betinget, dvs at den ikke er avhengig av hvor langt hovedmannen har kommet. En medvirker kan således dømmes for medvirkning til en forbrytelse selv om hovedmannen ikke har kommet på at han skal begå forbrytelsen engang. Dette kan tenkes dersom han eksempelvis driver en psykisk medvirkning.

Det har derimot vist seg i praksis at dette medvirkningstillegget ikke begrenser mye de kriminelle handlingene. Det er mulig at kunnskapen om rekkevidden av medvirkningsansvaret blant legmenn er for lav. Mange tror ikke de kan bli tatt så lenge de ikke selv har utført en straff bar handling. Samtidig vet mange at oppdagelsesrisikoen er lav, og det samme er resursene til politiet, slik at en medvirkning sjelden vil prioriteres. Dette er grunner for at andre straffebud legger opp til at slike forberedende eller medvirkende handlinger skal være selvstendige forbrytelser. De samme hensynene gjør seg gjeldende innen cybercrime.

Dette leder til spørsmålet rundt skyldkravet i bestemmelsene. Etter konvensjonens ordlyd skal det foreligge en spesiell hensikt om å bryte en av bestemmelsene i ar 2-5. Et medvirkningsansvar måtte tilfredsstille kravet om hensikt også hos medvirkeren. Etter § 145b gjelder kun alminnelig forsett. Med slikt forsettkrav er bevisspørsmålet mindre problematisk. Da vil man kunne holde gjerningsmannen ansvarlig for med rimelig sikkerhet å ha holdt det som sannsynlig at noen andre kunne benytte dette utstyret til straffbare handlinger. Dersom spredningen er ulovlig vil dette ha en større individualpreventiv virkning enn trusselen om medvirkningstillegget. Kunnskapen om slike tillegg er ikke så utbredt i alle felt, samtidig som at bevisspørsmålet blir vanskeligere. Jeg mener også at det kan virke mer vilkårlig for enkeltmennesker å bli straffet for medvirkning til en forbrytelse han ikke visste om ville bli begått, eller av hvem, enn å gjøre selve denne medvikende handlingen straffbar i seg selv.

Konvensjonen setter i punkt 1 første setning et krav om at statene skal kriminalisere "*følgende forsettlige og urettmessige*" handlinger. Det settes her opp et krav om alminnelig forsett, og det presiseres at man må grense mot de handlinger som er rettmessige av andre årsaker. Det er et gjennomgående tilleggskrav at handlingen må være uberettiget. Dette er for å skille ut de tilfellene der det foreligger en avtale eller en annen tillatelse med hjemmel annet steds fra. Selv om en handling objektivt passer inn i gjerningsbeskrivelsen er det ikke meningen å ramme rettmessige handlinger som forskning, eller inntreden med spesiell tillatelse.

Videre er det viktig å merke seg at konvensjonen legger opp til at man kun skal ramme den som handler med en spesiell hensikt om å begå en straffbar handling. Dette gjelder de straffbare handlingene som er beskrevet i art 2-5. Som en andre presisering av dette hensiktskravet er det satt opp et eget punkt 2, som bestemmer at hele punkt 1 av bestemmelsen ikke skal anvendes der det ikke er påvist hensikt om å begå en av de straffbare handlingene i art 2-5. Forskjellen mellom alminnelig forsett og hensiktskravet er at ved hensikt er det målet med handlingen å gjennomføre en straffbar handling. Ved vanlig

forsett er det tilstrekkelig om gjerningsmannen har holdt det for overveiende sannsynlig at noen vil bruke for eksempel passordene til noe kriminelt, eller at det straffbare vil inntre.

I den ”explanatory report” som foreligger fra Europarådet uttrykkes det at det kreves hensikt og urettmessighet for å unngå overkriminalisering. Det settes opp som krav at man både skal ramme det generelle forsett angående handlingene, og den spesifikke hensikt om å bryte en av artiklene 2-5. Andre kriminelle handlinger skal ikke rammes av denne bestemmelsen. Det skal ligge i ordet urettmessig at de fleste former for slik befatning ikke skal rammes så lenge det kan dokumenteres at det er med rett det foregår. Dersom man har tillatelse fra eier, handler i forskningsøyemed eller lignede. Handlingene i seg selv er ikke straffbare uten den onde hensikt.

Det argumenteres mye med at å utvide straffeansvaret til også å gjelde forberedende handlinger er uheldig fordi det blir en sinnelagsstrafferett. Det er bare aktuelt å straffe der det foreligger et forsett om å bryte en av nærmere bestemte forbrytelser. Hvorvidt dette forsettet foreligger eller ikke kan være vanskelig å påvise.

Departementet viser i sin utredning om dette til bakgrunnsretten og den generelle lære om at forberedelse ligger for langt unna en konkret visning av den forbryterske vilje til at den burde straffes. De legger vekt på at gjerningsmannen ikke enda har bestemt seg, og at det er stor sannsynlighet at han ikke vil gjennomføre når det kommer til stykket. Dette kan igjen føre til flere uriktige domfellelser. Departementet viser til, som eksempel, at et innkjøp i en jernvarehandel er en lovlig affære, men dersom man skal bruke innkjøpene til noe kriminelt vil det være en forberedelse på en straffbar handling. De presiserer imidlertid hvordan dette kan være annerledes når det gjelder kjøp av dataprogrammer eller lignende med et meget begrenset lovlig virkeområde. Det er innenfor denne oppgaven kun meningen å ramme befatning med datarelatert utstyr og programmer. I vårt tilfelle kan vi sammenligne med det å kjøpe seg hackerutstyr, noe som er en lovlig affære i dag. Hvorvidt dette blir en kriminell handling vil ikke være totalt avhengig av gjerningsmannes forsett om hva det skal brukes til. Utstyret må nemmelig være ”særlig egnet til å brukes i en straffbar forbrytelse”, og det

må ha liten annen egenverdi. Dersom disse to kravene til objektet er oppfylt, er det lite problematisk å definere det ulovlige fra det lovlige.

Departementet kom til den konklusjon at et hensiktskrav vil gjøre det vanskelig bevismessig å straffefølge slike handlinger. Man må da skaffe et motiv for gjerningsmannen og bevise dette. Det samme var konklusjonen i datakrimutvalget og senere i Stortinget.

Jeg er også kommet til den konklusjon at reglene om at befatningen må være uberettiget, samt at den må være forsettelig, er tilstrekkelig. Dette samsvarer godt med norsk rettstradisjon. Handlingene blir dermed gjort til spesielle straffebud. Det er ikke noe krav om at de blir gjennomført med en spesiell hensikt om å begå andre straffbare handlinger. Så lenge befatningen er uberettiget, og gjerningsmannen handler med forsett slik at han oppfyller gjerningsbeskrivelsen, kan han straffes. Bestemmelsen bør altså følge det alminnelige oppsettet i straffeloven, nemlig at den omfattes av § 21 om at kun forsettelige handlinger skal rammes med mindre noe annet er sagt eller utvetydig forutsatt.

Konklusjonen av denne gjennomgangen av hva som ikke er inkorporert av art 6 i norsk rett viser at dette bør gjennomføres. Dette bør gjøres først og fremst fordi Norge ved å signere konvensjonen også har signert for denne artikkelen, som anbefaler oss å kriminalisere disse handlingene. De andre landene som også har signert konvensjonen, deriblant våre naboland, har ratifisert denne på en meget tilfredsstillende måte. Norge henger således etter på dette feltet. Dette kan føre til at Norge blir en ”data haven” for de kriminelle, fordi reglene her ikke rekker så langt som i andre europeiske land.

6.2 **Hvordan bør resten av art 6 utformes?**

Resten av art 6 kan inkorporeres direkte gjennom vedtakelsen av den ordlyden som er inntatt i Ot.prp. nr.40 (2004 – 2005)[32]. Denne ordlyden er den offisielle norske versjonen. Europarådet har uttalt at de anbefaler den Rumenske modellen, som er en eksakt implementering av ordlyden i konvensjonen.

Det forslaget som ble fremmet av justisdepartementet i Ot.prp.nr. 40 (2004 – 2005) er et forslag som har vunnet frem etter vedtakelsen av § 145b.

Den lyder som kjent slik:

"*den som uberettiget fremstiller, anskaffer, besitter eller gjør tilgjenglig for andre*

c) passord eller andre data som kan gi tilgang til et datasystem, eller

d) dataprogrammer eller andre innretninger som er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer straffes med bøter eller fengsel inntil 6 måneder eller begge deler"

Medvirkning vil rammes etter § 15 i den nye straffeloven, og forsøk etter § 16.

Forslaget er gitt støtte av Stein Schjølberg, Sorenskriver i Moss tingrett og pioner på datakriminalitetens område[33]. Han inntar den samme ordlyden i sitt lovforslag fra mai 2007.

I dette forslaget foreslår han å samle alle bestemmelsene om datakriminalitet i ett kapittel, som han kaller kap 23 a - Vern av data, informasjon og informasjonsutveksling.

§ 23 a – 1: om uberettiget tilgang til lagrede data

§ 23 a – 2: om dataavlytting

§ 23 a – 3: om dataskadeverk

---

[32] s 38 flg i proposisjonen inneholder den offisielle norske versjonen, også inntatt i denne oppgavens punkt 3.2.

[33] se for øvrig han bok: *Cybercrime - straffbare handlinger mot den alminnelige fred og orden i cyberspace*

§ 23 a – 4: om systemskadeverk

§ 23 a – 5: om spredning av tilgangsdata og hackerverktøy lyder

§ 23 a – 6: om forberedelseshandlinger

kap 31 - om vern av tilliten til dokumenter og penger

Ordlyden i § 23a – 5 er den samme som forslaget fra justisdepartementet. Den dekker art 6 i konvensjonen.

Etter min mening er denne ordlyden bedre enn den som art 6 bruker. Forskjellen ligger i befatningsformene og hvilke straffbare handlinger befatningen med utstyret kan føre til.

Når det gjelder befatningsformene nevnes disse fire: ”fremstiller, anskaffer, besitter eller tilgjengeliggjør for andre…”
Dette er færre enn hva konvensjonen legger opp til. Disse fire befatningsformene dekker likevel på en tilfredsstillende måte det som skal rammes etter konvensjonen. Ordet ”besitter” er nevnt i bokstav b i konvensjonen og utgjør et eget punkt. Dette virker unødvendig, ettersom denne befatningsformen kan listes opp sammen med de andre befatningsformene. Konvensjonens befatningsformer overlapper hverandre, og dette gjør den uoversiktlig. For det første kan alle befatningsformene dekkes av disse fire ordene. Ettersom ordene salg og distribusjon ble antatt å dekkes tilfredsstillende av ordet tilgjengliggjøring i § 145b kan man i alle fall si at de andre formene dekkes av de fire som foreslås i proposisjonen. For det andre er det slik at dess flere befatningsformer som nevnes, dess vanskeligere er det å innsubsumere noe som ikke er nevnt. Dersom man kun nevner noen utvalgte, få former, som kan omfatte flere andre former, vil man kunne oppnå større oversiktlighet. Samtidig åpner dette for muligheten til å tilpasse bestemmelsen den utvikling som skjer. Dersom nye metoder for befatning utvikles kan disse innsubsumeres under bestemmelsen.

Når det gjelder det objektive gjerningsinnholdet som nevnes spesielt er dette helt likt det som nevnes i konvensjonen. Det sentrale er om disse passordene og innretningene er særlig

egnede til å begå straffbare handlinger mot data eller datasystemer. Dette kan kanskje tolkes noe videre enn den ordleggingen som konvensjonen bruker ”*…utviklet eller tilpasset hovedsakelig i den hensikt å begå en av de straffbare handlingene i art 2-5”* Det er godt mulig at hvorvidt utstyret har andre legitime anvendelsesområder får mindre betydning her. I konvensjonens ordlyd ser det ut som at den skadevoldende egenskapen må være hovedformålet. At den skal være særlig utviklet for en slik bruk viser tydelig at utstyr med andre formål ikke inngår. I Schjølbergs og departementets forslag trenger utstyret kun å være særlig egnet. Dette utelukker ikke andre formål også, men kun at den passer særlig godt til slike formål. Dette gir større frihet med hensyn til hva som omfattes, og man er henvist til å se mer helhetlig på situasjonen.

Når det gjelder hvilke straffbare handlinger dette utstyret skal være særlig egnet til å begå nevner forslaget generelt ”*straffbare handlinger som retter seg mot data eller datasystemer*”. Kriteriet er altså kun at det skal dreie seg om datarelaterte brudd. I konvensjonen er det brudd på nærmere angitte bestemmelser som rammes. Dette har stor faktisk betydning med hensyn til den utvikling som skjer innen feltet. Nye forbrytelser kommer til. En forberedelse på disse vil ikke rammes etter konvensjonens bestemmelser, mens etter forslaget vil det kunne rammes.

Det forslaget som ble lagt frem av justisdepartementet og Schjølberg ivaretar derfor bedre hensynene til oversiktlighet og fleksibilitet i lovverket. Det kan derimot diskuteres om ikke dette bør gjøres enda mer fleksibelt, slik at det rekker enda videre. Dette kan gjøres ved å innføre en generell forberedelsesregel innen dette feltet, enten i tillegg til dette forslaget eller i stedet for det.

7 EN GENERELL REGEL OM DET FORBEREDENDE ANSVARET

7.1 Bør ansvaret være mer generelt?

Her skal jeg se på om ikke det kan være fruktbart å ramme videre enn det art 6 i konvensjonen legger opp til. Det kan være ønskelig å utvide ansvaret enda mer enn det som kommer frem av justisdepartementets og Schjølbergs forslag. Dette forslaget dekker konvensjonens art 6 på en mer enn tilfredsstillende måte, men det kan fortsatt være ønskelig med større fleksibilitet med hensyn til den utvikling som vil skje.

Justisdepartementets forslag innebærer som sagt også en bedre måte å ramme befatningsformene på enn den konvensjonen legger opp til. De sammenfatter noen av formene i samme ord, slik at det blir noen færre former. I denne delen skal jeg vurdere en forlengelse av forberedelsesansvaret. Den ytterste generalitet vil kunne være å ramme alle befatningsformer av alle typer utstyr som et ledd i enhver form for straffbar handling. Visse begrensninger må til for ikke å ramme langt utover datakriminalitetens område. Jeg skal se nærmere hvordan man kan begrense det og på hvilke konsekvenser en slik utvidelse på alle fronter kunne ha.

Det første spørsmålet i denne delen er således hvorvidt man kan simplifisere oppramsingen av befatningsformer til å ramme all befatning. Det er selvfølgelig ønskelig å videreføre reservasjonen om at befatningen må være urettmessig, slik at den ikke har hjemmel i annen lov eller avtale. Man kan bruke ordene ”all befatning” eller ”enhver befatning”. Dette ville føre til større frihet under subsumeringen. Jo mer spesifikk bestemmelsen er, jo vanskeligere er det å tolke flere former for befatning inn under bestemmelsen. Dersom man føyer til nye befatningsformer etter hvert som utviklingen gjør det påkrevd snevrer man inn fleksibiliteten av bestemmelsen. Lovverket ville etter hvert bli meget omfattende og uoversiktlig. Dette strider mot viktige hensyn i forhold til legaliteten av bestemmelsene. Dersom man omfatter alle former for befatning vil det ikke være noen begrensninger. Den

nærmere presiseringen av hva som er lovlig og hva som ikke er det vil være avhengig av skjønn og utviklingen i teknologien og i rettspraksis.

Dette leder også til neste poeng, nemlig at det sentrale etter denne modellen ikke er hvilke befatningsformer som brukes, men hvilket objekt gjerningsmannen befatter seg med. Konvensjonen nevner for det første innretning, herunder et dataprogram, og for det andre passord og adgangskoder. Det sentrale for innretningene er at de utviklet eller tilpasset hovedsakelig til å begå kriminelle handlinger. Departementet tolker dette til å omfatte enhver logisk eller fysisk innretning som er særlig egnet ved overtredelsen av artikkel 2-5 er omfattet. Når det gjelder punkt ii) mener de at dette bør omfatte alle former for data som kan gi tilgang til hele eller deler av et datasystem, typisk et passord.

Et prinsipp er at man holder den objektive gjerningsinnholdet så teknologisk nøytral som mulig, ettersom man ønsker å møte utviklingen. Man bruker ordet data fremfor informasjon, for dette er ikke noe som kan lagres eller overføres i seg selv, den oppstår først i menneskets bevissthet når data prosesseres. Data er heller ikke en gjenstand. Lagringsmediene kan være det, men data i seg selv er immaterielle verdier i form av magnetiske impulser.

Dette kan gjøres enklere og mindre begrenset, ved å ramme alt datateknologisk utstyr, som er særlig egnet til å bruke som hjelpemiddel til å begå straffbare handlinger. Det sentrale bør således ikke være å definere hvilke adgangskoder eller hvilket utstyr som rammes, men hvorvidt dette er særlig egnet til å anvende som hjelpemiddel i en straffbar handling. Jeg viser for øvrig til drøftelsen i forrige kapittel, og presiserer igjen at det må dreie seg om utstyr med liten egenverdi utover å brukes i kriminell sammenheng. Man begrenser heller ikke utstyret til kun å ramme det som er utviklet hovedsakelig i den hensikt å begå en straffbar handling, men omfatter kun det som er særlig egnet. Dette betyr, jamfør drøftelsen over, at utstyret kan ha andre formål i tillegg uten at det utelukker straffbarhet. De objektene som har flere bruksområder vil kunne rammes, selv om disse ikke er like selvfølgelig omfattet som de objektene som kun har denne funksjonen.

I dag rammes ingen dataprogrammer eller innretninger, selv om de er utviklet kun for å begå straffbare handlinger. Dette står i motsetning til andre typer objekter, som våpen, sprengstoff etc, som er ulovlig fordi de har en skadevoldende evne i kombinasjon med liten egenverdi. Datateknologiske innretninger kan åpenlyst kjøpes, selges og spres. Og dette gjøres i stort omfang. Dette gjør det umulig å holde kontroll på hvem som sitter på stor makt, kunnskap og utstyr, til å gjøre stor skade. Forberedende handlinger, som for eksempel elektronisk kartlegging, er mer nærgående og mer farlig enn for eksempel en forberedelse til fysisk innbrudd. I begge tilfeller kan man sirkle rundt et "vindu" for å planlegge entring. Men man er psykologisk og faktisk nærmere ved den elektroniske kartleggingen. Det står ikke igjen mange fysiske handlinger før man kan entre her. I tillegg har man ofte færre motforestillinger mot å sitte hjemme og taste enn å bevege seg ut i mørket for å begå et innbrudd.

Dette leder inn på det tredje og siste vurderingstemaet i straffebudet, nemlig når slike handlinger er straffbare. I konvensjonen gjelder det kun der handlingene er en forberedelse til brudd på art 2-5. Dette begrenser det straffbare området mye, og gjør det definerbart.

Utviklingen innen feltet datakriminalitet tilsier derimot at nye former for kriminalitet må møtes. Det utvikles nye metoder hele tiden, og de kriminelle handlingene begrenser seg ikke til å gjelde de som omfattes av art 2-5. Phishing, pharming, botnets, spam og spyware er noen av disse nye metodene som er utviklet den siste tiden. Og utviklingen kommer ikke til å stoppe her. Det er nødvendig å omfatte forberedelse på disse handlingene, og på andre handlinger som utvikles over tid. Andre mer fysiske kriminelle handlinger kan utføres ved hjelp av datateknologi. Dette kan gjelde for eksempel terror, som ikke er noen datarelatert forbrytelse. Men som beskrevet over kan data brukes som ledd i en straffbar handling, som ved cyberterrorism. Forberedelse på slike handlinger bør også rammes. Det må holdes i minne at cybercrime er enhver straffbar handling hvor data utgjør et ledd, enten som mål, middel eller arena for gjennomføringen.

Dersom man omfatter forberedelse på alle straffbare handlinger, der data utgjør en del av denne forberedelsen, som straffbar forberedelse vil man kunne oppnå fleksibilitet og den forebygging som er ønskelig.

7.2 Hvordan kan denne utvidelsen manifestere seg?

Straffebudet kan altså utvides til å gjelde enhver befatning, med enhver type utstyr som er særlig egnet til å begå enhver type straffbar handling, så lenge det dreier seg om datakriminalitet.

Oppsettet som danskene har valgt kan være et eksempel, selv om denne også favner alle rettsområder. Den rammer alle handlinger som sikter til å fremme eller bevirke utførelsen av en straffbar handling. En slik regel kan plasseres i den alminnelige del i straffeloven. Dette ville føre for langt i forhold til diskusjonen rundt cybercrime, slik at man må definere anvendelsesområdet noe. Et liknende oppsett innen datakriminologi kunne være å ramme alle handlinger som sikter til å fremme eller bevirke utførelsen av en kriminell handling med bruk av datateknologi. En slik bestemmelse kunne også plasseres i den alminnelige del av straffeloven.

I Sverige er det objektive gjerningsinnholdet definert noe mer med vurderingstemaet særlig egnet til å brukes som hjelpemiddel ved den forbrytelse. § 2 i Brottsbalken rammer ”*något som är särskilt ägnat att användas som hjälpmedel vid ett brott***”.**
Ordet ”något” omfatter alt. Samtidig begrenser den noe anvendelsesområdet, slik at ikke hele vurderingstemaet koker ned til gjerningsmannens hensikter. Den gir et objektivt holdepunkt til vurderingen. Bestemmelsen gjelder ikke kun for datarelaterte forbrytelser, men den er utformet nettopp med dette i tankene.

Som en neste mulighet kan man plassere bestemmelsen i kapittelet om cybercrime, som den første bestemmelsen i dette kapittelet, eller i forbindelse med bestemmelsen om ”spredning av tilgangsdata og hackerverktøy”. Man kan slå fast at alle former for

forberedelse på kriminelle handlinger ved bruk av data som mål, middel eller arena straffes som egne forbrytelser. På denne måten møter man den utvikling som forutsettes å skje innen datateknologiens område. Man definerer ikke nærmere hvilke straffbare handlinger man mener, men sier at alle forberedende handlinger hvor man bruker datateknologi som hjelpemiddel til en annen straffbar handling rammes. I motsetning til det forslaget som ble lagt frem av datakrimutvalget vil en slik generell regel kunne møte den utvikling som skjer.

Stein Schjølberg sitt forslag gjør nettopp dette. Han foreslår å ha en generell regel i tillegg til regelen om spredning av tilgangsdata og hackerverktøy, og fanger opp de tilfellene som ikke omfattes av denne.

Schjølberg har lagt frem et forslag som lyder:
§ 23 a – 6: enhver befatning med data i et datasystem som er særlig egnet til å anvendes som hjelpemiddel til en straffbar handling, straffes som forberedelse til straffbar handling.

Denne bestemmelsen gjelder alle former for befatning. Utstyret er kun definert som ”data”, noe som er tilstrekkelig begrenset men likevel fleksibel. Dataene må være særlig egnet til å begå straffbare handlinger. Den omfatter alle former for straffbare handlinger, og dette straffes som en selvstendig forbrytelse.

Stein Schjølberg sitt forslag er derfor fleksibelt nok til å møte utviklingen, samtidig som den presiserer anvendelsesområdet. Med tillegg av § 23a – 5 dekker dette forberedelseshandlinger innen datakriminalitetens område.

8 FORSLAG TIL GJENNOMFØRING AV FORBEREDELSESANSVARET INNEN DATAKRIMINALITET

8.1 En ytterligere utvidelse og generalisering av reglene

Jeg vil i denne delen foreslå en siste måte å ramme forberedelseshandlinger innen datakriminalitet på.

Jeg mener at Schjølberg sitt forslag kan videreføres, slik at det blir mer generelt og fleksibelt.

§ 23a – 5 inneholder to forskjellige gjerningsbeskrivelser. Det ene er uberettiget befatning med passord og andre koder, som er straffbart i seg selv. Det andre er uberettiget befatning med dataprogrammer og andre innretninger, som er straffbart der disse er særlig egnet til å brukes som hjelpemiddel i en straffbar handling.

Når det gjelder befatningsformene for begge typene av utstyr er det altså etter min mening ikke nødvendig å nevne alle de fire formene ”fremstiller, anskaffer, besitter eller gjør tilgjengelig for andre”. Dersom man bruker ordene ”enhver befatning”, slik han foreslår det selv i § 23a – 6, vil man omfatte det som skal med, men samtidig andre former for befatning som utvikles senere. I sammenheng med kravet om urettmessighet vil dette begrense anvendelsesområdet tilstrekkelig. Det holder å ramme enhver urettmessig befatning, både for passordene og for dataprogrammene.

Når det gjelder bokstav b) om dataprogrammer og andre innretninger kan denne konsumeres av gjerningsbeskrivelsen i § 23a – 6. Ordene ”enhver befatning” kan være dekkende også her. Objektet data i datasystem, som er særlig egnet til å begå en straffbar handling, kan konsumere ordene dataprogrammer eller andre innretninger. I tillegg kan begge straffes som forberedelse til straffbar handling. Å kriminalisere spredning av

hackerverktøy kan være overflødig dersom man kriminaliserer enhver befatning med slikt datarelatert utstyr som kan anvendes som hjelpemiddel i en straffbar handling. På samme måte som lovforslaget i NOU 2007:2 fremstår som lite fleksibel når den kriminaliserer spesielle forberedelsesdelikt for seg, kan man si det samme om § 23a – 5 b) i Schjølberg sitt forslag. Det virker unødvendig å ramme den samme handling to ganger i samme kapittel, først som en egen bestemmelse og senere som en del av en mer generell bestemmelse.

8.2 Hvordan skal en slik utvidelse manifestere seg?

Mitt forslag til utforming av bestemmelsene om forberedelseshandlinger innen datakriminalitet er derfor slik:

§ 23a – 5: spredning av tilgangsdata:
Enhver uberettiget befatning med passord eller andre data som kan gi tilgang til et datasystem straffes med bøter eller fengsel i inntil 1 år eller begge deler.
Grov spredning straffes med fengsel inntil 3 år. Ved avgjørelsen av om overtredelsen er grov, skal det blant annet legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen skaper fare for betydelig skade. Medvirkning straffes på samme måte.

§ 23a – 6:
Enhver befatning med data i datasystem som er særlig egnet til å anvendes som hjelpemiddel til en straffbar handling, straffes som forberedelse til straffbar handling.

Dette forslaget rammer det samme som Schjølberg sitt forslag. Forskjellen er altså kun at jeg foreslår å ramme alle former for befatning også for passord og andre data, og at jeg foreslår å innbefatte § 23a – 5 b) i § 23a – 6.

9 VEDLEGG

9.1 Litteraturliste

Bøker

Husabø, Erling Johannes: *Straffeansvarets Periferi*, Bergen 1999, Universitetsforlaget

Andenæs, Johs.: *Alminnelig Strafferett*, 5 utg, 2005, Universitetsforlaget

Schjølberg, Stein: *Cybercrime – straffbare handlinger mot den alminnelige orden og fred i cyberspace*, 2006, www.cybercrimelaw.net

Utredninger og proposisjoner

NOU 1985:31 ”Datakriminalitet”

NOU 2002:4 “Ny Straffelov”
Ot.prp nr 90 (2003-2004) “Straffeloven”

NOU 2003:27 del I ”Lovtiltak mot datakriminalitet”
Ot.prp nr 40 (2004-2005) “om lov om endringer I straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet)”

Innst. O nr 53 (2004-2005) ”innstilling fra justiskomiteen om …(lovtiltak mot datakriminalitet)”
Besl.O.nr.48 (2004-200) ”lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet)”

NOU 2007:2 del II ”lovtiltak mot datakriminalitet”

Høringsnotat fra Lovavdelingen, april 2007, ”forslag til et kapittel i ny straffelov med straffebud mot terrorhandlinger og terrorrelaterte handlinger og spørsmålet om ratifikasjon av Europarådets konvensjon om forebygging av terrorisme”

Folkerettslige forpliktelser

Convention on Cybercrime, Europarådets konvensjon om bekjempelse av datakriminalitet av 23.11.2001
”Explanatory Report”, den forklarende rapporten til konvensjonen, punkt 71-78

Council og Europe Convention on the Prevention of Terrorism, Europarådets konvensjon om bekjempelsen av terror av 16.05.2005

Internettsider

www.cybercrimelaw.net
www.wikipedia.com
www.regeringen.se
www.regjeringen.no
www.stortinget.no
www.lovdata.no
www.danmark.dk

www.domstol.dk
www.justisministeriet.dk
www.conventions.coe.int

Utenlandsk rett

Svensk rett:
Den svenske straffeloven, Brottsbalken 23 kapittel
SOU 1996:185
Prop 2000/01:85
DS 2005:6

Dansk rett
Den danske straffeloven, §21
Betænkning nr 1417, 2002
Dom fra København Byrett av 11.04.2007 om medvirkning til terrorisme

Andre verk om datakriminalitet

Schjølberg, Stein: ”Terrorism in Cyberspace – Myth or reality?” (se cybercrimelaw.net)
Solstad, Berit Børset: foredrag om datakriminalitet fra 20 sept 2007.

Tidligere masteroppgaver i jus om datakriminalitet

Sunde, Lars Christian, “Elektronisk dokumentfalsk” vår 2004
Samnøen, Audun, ”Om uberettiget besittelse av datavirus og hackerverktøy”, høst 2006
Maana, Joo Arne, ”Overgrep mot barn i Cyberspace”, vår 2007.

9.2 Vedlegg 1 – europarådets konvensjon om bekjempelsen av cybercrime

Convention on Cybercrime

Budapest, 23.XI.2001

Additional Protocol
Explanatory Report
Français

Non-official translations *(various formats)*:
Arabic *(Source : INTERPOL)*
Español
Português & Relatório explicativo

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a

computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence

established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of

Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse

mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it

shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall

then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect

of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three

months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as

referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

9.3 Vedlegg 2 – Europarådets konvensjon om bekjempelsen av terror

Convention on Cybercrime

Budapest, 23.XI.2001

Additional Protocol
Explanatory Report
Français

Non-official translations *(various formats)*:
Arabic *(Source : INTERPOL)*
Español
Português & Relatório explicativo

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and

neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in

the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply

the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the

request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to

believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles

governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.